INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

January 6, 2023
Ref: DODOIG-2022-000314

SENT VIA EMAIL TO: john@greenewald.com
Mr. John Greenewald
The Black Vault, Inc.
27305 W. Live Oak Road, Suite 1203
Castaic, CA 91384

Dear Mr. Greenewald:

This responds to your Freedom of Information Act (FOIA) request for all emails (including all attachments) sent to/from (bcc'd or cc'd) Acting Inspector General Sean O'Donnell, which contain the keywords unidentified aerial phenomena and/or unidentified aerial phenomenon and/or UAP and/or UAPTF and/or UFO and/or unidentified flying object and/or AOIMSG, from April 6, 2020, through the date of processing this request. We received your request on January 4, 2022, and assigned it case number DODOIG-2022-000314. By email dated March 22, 2022, you agreed to scope out all publicly available news articles not containing commentary.

The Mission Support Team conducted a search and located records responsive to your request. Upon review, we determined that the attached 406 pages are appropriate for release in part pursuant to the following FOIA (5 U.S.C. § 552) exemptions:

- (b)(5), which pertains to certain inter-and intra-agency communications protected by the deliberative process privilege. The purpose for withholding such recommendations is to encourage the free and candid exchange of opinions and advice during the decision-making process. In applying the foreseeable harm standard, we determined that disclosure of this information is likely to diminish the candor of agency deliberations in the future; and

- (b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy.

Our review included consideration of the foreseeable harm standard, as stated in DoDM 5400.07. Under this standard, the content of a particular record should be reviewed and a determination made as to whether the DoD Component reasonably foresees that disclosing it, given its age, content, and character, would harm an interest protected by an applicable exemption.

If you consider this an adverse determination, you may submit an appeal. Your appeal, if any, must be postmarked within 90 days of the date of this letter, clearly identify the

determination that you would like to appeal, and reference to the FOIA case number above. Send your appeal to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500, or via facsimile to 571-372-7498. However, please note that FOIA appeals can only examine adverse determinations concerning the FOIA process. For more information on appellate matters and administrative appeal procedures, please refer to 32 C.F.R. Sec. 286.9(e) and 286.11(a).

You may contact our FOIA Public Liaison at FOIAPublicLiaison@dodig.mil, or by calling 703-604-9785, for any further assistance with your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, MD 20740-6001, email at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one's own records).

If you have any questions regarding this matter, please contact Ms. Derrica Stone at 703-604-9775 or via email at foiarequests@dodig.mil.

Sincerely,

Searle Slutzkin
Division Chief
FOIA, Privacy and Civil Liberties Office

Attachment(s):
As stated

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: **http://www.theblackvault.com**

From	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @DODIG.MIL>
To	'(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "Stebbins, Steven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, (b) (6) @epa.gov" <(b) (6) @epa.gov>, '(b) (6) @epa.gov" <(b) (6) @epa.gov>, '(b) (6) " <(b) (6) @epa.gov>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Cc	'(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Subject	OLAC Weekly
Date	Fri, 23 Apr 2021 15:37:03 +0000
Message-Id	<526811352ba34f08a5663f3e64fd0c07@DODIG.MIL>

Agenda attached for Apr 26th meeting.
Weekly OLAC meeting with Acting IG.
Jabber Conf ID: (b) (6) , Pass: (b) (6) or Dial-in: (b) (6) , ID: (b) (6) , Pass: (b) (6)

.....

Attachment Name : OLAC Weekly Meeting 04.26.21.pdf

OLAC Weekly Meeting Agenda
Monday, April 26, 2021 @ 10:00 a.m.
~~**For Official Use Only**~~

Dial-in Info
Jabber Conf ID: [redacted], **Pass:** [redacted] **or**
Dial-in: [redacted], **ID:** [redacted], **Pass:** [redacted]

MATTERS FOR DISCUSSION

- **SAR** – status;
- [redacted];
- [redacted];
- [redacted];
- **Unidentified Aerial Phenomena** – roll out confirmation;
- [redacted];
- [redacted];
- **CIGIE/GAO Financial Statement Audit Conference** – publishing banner and about two-day virtual conference on May 17 and 18;
- [redacted];
- **Public Service Recognition Week**— discussion strategy; and
- **Agency Financial Report** – status.

From	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @DODIG.MIL>
To	'(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "Stebbins, Steven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) @epa.gov" <(b) (6) @epa.gov>, '(b) (6) @epa.gov" <(b) (6) @epa.gov>, '(b) (6) " <(b) (6) @epa.gov>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Cc	'(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>
Subject	OLAC Weekly
Date	Fri, 30 Apr 2021 15:41:05 +0000
Message-Id	<4b2348ba69bd4262a4d58f11ef42fd43@DODIG.MIL>

Agenda with attachment attached for the May 3rd OLAC Weekly meeting.
Weekly OLAC meeting with Acting IG.
Jabber Conf ID: (b) (6) , Pass: (b) (6) or Dial-in: (b) (6) , ID: (b) (6) , Pass: (b) (6)

.....

Attachment Name : 2021-40-28 CEG to DOD (JEDI Jan 1 follow up) (fd).pdf

.....

Attachment Name : OLAC Weekly Meeting 05.03.pdf

OLAC Weekly Meeting Agenda
Monday, May 3, 2021 @ 10:00 a.m.
~~**For Official Use Only**~~

Dial-in Info
Jabber Conf ID: (b) (6) **, Pass:** (b) (6) **or**
Dial-in: (b) (6) **, ID:** (b) (6) **, Pass:** (b) (6)

MATTERS FOR DISCUSSION

- **Unidentified Aerial Phenomena** – May 3 and 4 roll out confirmation;
- (b) (5) ;
- (b) (5) ;
- (b) (5) ;
- **Public Service Recognition Week**— discussion strategy; and
- **Agency Financial Report** – status.

From	"Stebbins, Steven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>
To	'(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL> , '(b) (6) @epa.gov" <(b) (6) @epa.gov>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) @epa.gov" <(b) (6) @epa.gov >, "O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>, "(b) (6) @epa.gov'" <(b) (6) @epa.gov>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "Mayo, Kelly P., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "Gorman, Carol N., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Hadjiyane, Paul, SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Subject	OLAC Update
Date	Tue, 4 May 2021 20:13:17 +0000
Message-Id	<c32921be0b5245d19e15a2e2e25a3781@DODIG.MIL>

Agenda and supporting documents attached to meeting invite for May 5th. Added the following to calendar invite for this meeting:
Sean O'Donnell
(b) (6)
Kelly Mayo
(b) (6) /Carol Gorman
Paul Hadjiyane/(b) (6)
OLAC Update weekly with Acting PDIG.
Jabber Conf ID: (b) (6) , Pass: (b) (6) or Dial-in: (b) (6) , ID: (b) (6) , Pass: (b) (6)

.....

Attachment Name : Letter to DOD OIG 05.04.21.pdf

.....

Attachment Name : Letter to AG Garland 05.04.21.pdf

.....

Attachment Name : Letter to Amazon 05.04.21.pdf

.....

Attachment Name : May 5 2021 Update Meeting Agenda.pdf

OLAC UPDATE Meeting Agenda
Wednesday, May 5 @ 10:00 a.m.
~~For Official Use Only~~

Jabber Conf ID: (b) (6) **, Pass:** (b) (6) **or**
Dial-in: (b) (6) **, ID:** (b) (6) **, Pass:** (b) (6)

Updates and Other Items for Discussion:

- (b) (5)
- **UAP** - Hill and media response; and
- (b) (5)

From	'(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>, "Stebbins, Steven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "Roark, Michael J., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Stone, Randolph R., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Cc	"Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Subject	FW: [Non-DoD Source] Pentagon watchdog opens new probe into military's handling of UFOs
Date	Tue, 4 May 2021 22:12:04 +0000
Message-Id	<b4001c4cf8e04f2dab6d5ce0aa8e1541@DODIG.MIL>

Good afternoon,
FYSA, below is a PoliticoPro article on the announced UAP evaluation:
Pentagon watchdog opens new probe into military's handling of UFOs
By Bryan Bender | 05/04/2021 02:20 PM EDT
The Pentagon's inspector general has launched an evaluation into the actions the military has taken to address the spate of UFO sightings in recent years involving high performance aircraft that have violated military airspace.
The probe comes as Congress awaits a public report, due next month, from a host of national security agencies on the issue, and as advocates complain<https://www.politico.com/news/2021/03/25/ufo-sightings-report-478104?source=email> that some departments and agencies are not fully cooperating by sharing data.
"The objective of this evaluation is to determine the extent to which the DoD has taken actions regarding Unidentified Aerial Phenomena (UAP)," Randolph Stone, assistant inspector general for evaluations on space, intelligence, engineering, and oversight, wrote in a Monday memo<https://media.defense.gov/2021/May/04/2002633947/-1/-1/1/D2021-DEV0SN-0116.000_REDACTED.PDF?source=email> to the heads of the military branches and other top military commanders and intelligence chiefs.
"We may revise the objective as the evaluation proceeds, and we will consider suggestions from management for additional or revised objectives," it added.
The memo was first reported by The Debrief.<https://thedebrief.org/inspector-general-launching-evaluation-of-the-pentagons-actions-with-ufos/?source=email>
It was not immediately clear who decided that the department's independent watchdog should take on the issue.
The Pentagon set up an Unidentified Aerial Phenomenon Task Force<https://www.defense.gov/Newsroom/Releases/Release/Article/2314065/establishment-of-unidentified-aerial-phenomena-task-force/?source=email> last year.
But one former top Pentagon intelligence official who has lobbied Congress to take more action on such sightings<https://www.youtube.com/watch?v=rO_M0hLIJ-Q&source=email> said on Tuesday that the IG's involvement is a positive step.
"You are looking at how is it possible that restricted military airspace is being routinely violated for months and years and nobody is informed in the Defense Department or the Congress and there is a complete system breakdown," said Christopher Mellon, former deputy assistant secretary of defense for intelligence. "That's a valid thing for them to investigate."

Very Respectfully,

(b) (6)
Legislative Affairs
Office of Legislative Affairs and Communications
DoD Office of Inspector General
(b) (6)

From	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6)@dodig.mil>
To	'(b) (6) OIG DoD" <(b) (6)@DODIG.MIL>, '(b) (6), OIG DoD" <(b) (6)@DODIG.MIL>, "Stebbins, Steven A., SES, OIG DoD" <(b) (6)@DODIG.MIL>, "Zola, Michael C., OIG DoD" <(b) (6)@DODIG.MIL>, '(b) (6)., OIG DoD" <(b) (6)@DODIG.MIL>, '(b) (6), OIG DoD" <(b) (6)@DODIG.MIL>, '(b) (6), OIG DoD" <(b) (6)@DODIG.MIL>, '(b) (6)@epa.gov" <(b) (6)@epa.gov>, '(b) (6)@epa.gov" <(b) (6)@epa.gov>, '(b) (6)" <(b) (6)@epa.gov>, '(b) (6)., OIG DoD" <(b) (6)@DODIG.MIL>, '(b) (6), OIG DoD" <(b) (6)@DODIG.MIL>
Cc	'(b) (6) OIG DoD" <(b) (6)@DODIG.MIL>
Subject	OLAC Weekly
Date	Fri, 7 May 2021 14:54:31 +0000
Message-Id	<55d05fac80994d3c961a2f3e6630fe57@DODIG.MIL>

Agenda for May 10th OLAC Weekly is attached.
Weekly OLAC meeting with Acting IG.
Jabber Conf ID:(b) (6), Pass:(b) (6) or Dial-in:(b) (6), ID:(b) (6), Pass:(b) (6)

.....

Attachment Name : OLAC Weekly Meeting 05.10.21 (final).pdf

OLAC Weekly Meeting Agenda
Monday, May 10, 2021 @ 10:00 a.m.
~~**For Official Use Only**~~

Dial-in Info
Jabber Conf ID: (b) (6) **, Pass:** (b) (6) **or**
Dial-in: (b) (6) **, ID:** (b) (6) **, Pass:** (b) (6)

MATTERS FOR DISCUSSION

- (b) (5)
-
-
- **UAP** – SASC and SSCI request for briefing;
- (b) (5) ;
- (b) (5) ;
- **MILDET Spotlight** – update; and
- (b) (5)

From	"(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>
To	"List .SESLIST" <(b) (6) @dodig.mil>
Cc	"(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>
Subject	UFOs regularly spotted in restricted U.S. airspace, report on the phenomena due next month
Date	Mon, 17 May 2021 08:53:21 +0000
Message-Id	<38823330c4bd458a91e13dd49b8eb20e@DODIG.MIL>

Good morning, all.
ICYMI, 60 minutes aired a segment last evening on UAP's that has spurred concern and interest by Congress and the DoD.
The segment is about 14 minutes long and may viewed on Chrome here,https://www.cbsnews.com/news/ufo-military-intelligence-60-minutes-2021-05-16/
[Transcript]
We have tackled many strange stories on 60 Minutes, but perhaps none like this. It's the story of the U.S. government's grudging acknowledgment of unidentified aerial phenomena- UAP-more commonly known as UFOs. After decades of public denial the Pentagon now admits there's something out there, and the U.S. Senate wants to know what it is. The intelligence committee has ordered the director of national intelligence and the secretary of defense to deliver a report on the mysterious sightings by next month.
Bill Whitaker: So what you are telling me is that UFOs, unidentified flying objects, are real?
Lue Elizondo: Bill, I think we're beyond that already. The government has already stated for the record that they're real. I'm not telling you that. The United States government is telling you that.
Luis Elizondo spent 20 years running military intelligence operations worldwide: in Afghanistan, the Middle East and Guantanamo. He hadn't given UFOs a second thought until 2008. That's when he was asked to join something at the Pentagon called the Advanced Aerospace Threat Identification Program, or "AATIP."
Lue Elizondo: The mission of AATIP was quite simple. It was to collect and analyze information involving anomalous aerial vehicles, what I guess in the vernacular you call them UFOs. We call them UAPs.
Bill Whitaker: You know how this sounds? It sounds nutty, wacky.
Lue Elizondo: Look, Bill, I'm not, I'm not telling you that, that it doesn't sound wacky. What I'm telling you, it's real. The question is, what is it? What are its intentions? What are its capabilities?
Buried away in the Pentagon, AATIP was part of a $22 million program sponsored by then-Senate Majority Leader Harry Reid to investigate UFOs. When Elizondo took over in 2010 he focused on the national security implications of unidentified aerial phenomena documented by U.S. service members.
Lue Elizondo: Imagine a technology that can do 6-to-700 g-forces, that can fly at 13,000 miles an hour, that can evade radar and that can fly through air and water and possibly space. And oh, by the way, has no obvious signs of propulsion, no wings, no control surfaces and yet still can defy the natural effects of Earth's gravity. That's precisely what we're seeing.
Elizondo tells us AATIP was a loose-knit mix of scientists, electro-optical engineers, avionics and intelligence experts, often working part time. They combed through data and records, and analyzed videos I ke this.
A Navy aircrew struggles to lock onto a fast-moving object off the U.S. Atlantic Coast in 2015.
Recently released images may not convince ufo skeptics, but the pentagon admits it doesn't know what in the world this is or this or this.
Bill Whitaker: So what do you say to the skeptics? It's refracted light. Weather balloons. A rocket being launched. Venus.
Lue Elizondo: In some cases there are simple explanations for what people are witnessing. But there are some that, that are not. We're not just simply jumping to a conclusion that's saying, "Oh, that's a UAP out there." We're going through our due diligence. Is it some sort of new type of cruise missile technology that China has developed? Is it some sort of high-altitude balloon that's conducting reconnaissance? Ultimately when you have exhausted all those what ifs and you're still left with the fact that this is in our airspace and it's real, that's when it becomes compelling, and that's when it becomes problematic.

Former Navy pilot Lieutenant Ryan Graves calls whatever is out there a security risk. He told us his F/A-18F squadron began seeing UAPs hovering over restricted airspace southeast of Virginia Beach in 2014 when they updated their jet's radar, making it possible to zero in with infrared targeting cameras.
Bill Whitaker: So you're seeing it both with the radar and with the infrared. And that tells you that there is something out there?
Ryan Graves: Pretty hard to spoof that.
These photographs were taken in 2019 in the same area. The Pentagon confirms these are images of objects it can't identify. Lieutenant Graves told us pilots training off the Atlantic Coast see things like that all the time.
Ryan Graves: Every day. Every day for at least a couple years.
Bill Whitaker: Wait a minute, every day for a couple of years?
Ryan Graves: Uh-huh.
Ryan Graves: I don't see an exhaust plume.
Bill Whitaker: You can sorta hear the surprise in their voices.
Ryan Graves: You certainly can. They seem to have broke character a bit and were just kind of amazed at what they were seeing.
Bill Whitaker: What do you think when you see something l ke this?
Ryan Graves: This is a difficult one to explain. You have rotation, you have high altitudes. You have propulsion, right? I don't know. I don't know what it is, frankly.
He told us pilots speculate they are one of three things: secret U.S. technology, an adversary's spy vehicle, or something otherworldly.
Ryan Graves: I would say, you know, the highest probability is it's a threat observation program.
Bill Whitaker: Could it be Russian or Chinese technology?
Ryan Graves: I don't see why not.
Bill Whitaker: Are you alarmed?
Ryan Graves: I am worried, frankly. You know, if these were tactical jets from another country that were hangin' out up there, it would be a massive issue. But because it looks slightly different, we're not willing to actually look at the problem in the face. We're happy to just ignore the fact that these are out there, watching us every day.
The government has ignored it - at least publicly - since closing its project "Blue Book" investigation in 1969. But that began to change after an incident off Southern California in 2004, which was documented by radar, by camera, and four naval aviators. We spoke to two of them: David Fravor, a graduate of the Top Gun naval flight school and commander of the F/A-18F squadron on the USS Nimitz; and flying at his wing, Lieutenant Alex Dietrich, who has never spoken publicly about the encounter.
Alex Dietrich: I never wanted to be on national TV, no offense.
Bill Whitaker: So why are you doing this?
Alex Dietrich: Because I was in a government aircraft, because I was on the clock. And so I feel a responsibility to s-- to share what I can. And it is unclassified.
It was November 2004 and the USS Nimitz carrier strike group was training about 100 miles southwest of San Diego. For a week, the advanced new radar on a nearby ship, the USS Princeton, had detected what operators called "multiple anomalous aerial vehicles" over the horizon, descending 80,000 feet in less than a second.
On November 14, Fravor and Dietrich, each with a weapons systems officer in the backseat, were diverted to investigate. They found an area of roiling whitewater the size of a 737 in an otherwise calm, blue sea.
Dave Fravor: So as we're looking at this, her back-seater says, "Hey, Skipper, do you..." And about that got out, I said, "Dude, do you, do you see that thing down there?" And we saw this little white Tic Tac-looking object. And it's just kind of moving above the whitewater area.
As Deitrich circled above - Fravor went in for a closer look.
Bill Whitaker: So you're sort of spiraling down?
Dave Fravor: Yep. The Tic Tac's still pointing north-south, it goes, click, and just turns abruptly. And starts mirroring me. So as I'm coming down, it starts coming up.
Bill Whitaker: So it's mimicking your moves?
Dave Fravor: Yeah, it was aware we were there.
He said it was about the size of his F/A-18F, with no markings, no wings, no exhaust plumes.
Dave Fravor: I want to see how close I can get. So I go like this. And it's climbing still. And when it gets right in front of me, it just disappears.
Bill Whitaker: Disappears?
Dave Fravor: Disappears. Like, gone.
It had sped off.
Bill Whitaker: What are you thinking?

Alex Dietrich: So your mind tries to make sense of it. I'm gonna categorize this as maybe a helicopter or maybe a drone. And when it disappeared. I mean it was just...
Bill Whitaker: Did your back-seaters see this too?
Alex Dietrich: Yeah.
Dave Fravor: Oh yeah. There was four of us in the airplanes literally watching this thing for roughly about five minutes.
Seconds later, the Princeton reacquired the target. 60 miles away. Another crew managed to briefly lock onto it with a targeting camera before it zipped off again.
Alex Dietrich: You know, I think that over beers, we've sort of said, "Hey man, if I saw this solo, I don't know that I would have come back and said anything," because it sounds so crazy when I say it.
Bill Whitaker: You understand that reaction?
Dave Fravor: I do. I've had some people tell me, you know, "When you say that, you can sound crazy." I'll be hon-- I'm not a UFO guy.
Bill Whitaker: But from what I hear you guys saying, there's something?
Alex Dietrich: Yes.
Dave Fravor: Oh there's, there's definitely something that... I don't know who's building it, who's got the technology, who's got the brains. But there's, there's something out there that was better than our airplane.
The aircrew filed reports. Then I ke the mysterious flying object, the Nimitz encounter disappeared. Nothing was said or done officially for five years, until Lue Elizondo came across the story and investigated.
Lue Elizondo: We spend millions of dollars in training these pilots. And they are seeing something that they can't explain. Furthermore, that informations being backed up on electro optical data, like gun camera footage. And b y radar data. Now, to me, that's compelling.
Inside the Pentagon his findings were met with skepticism. AATIP's funding was eliminated in 2012, but Elizondo says he and a handful of others kept the mission alive until finally, frustrated, he quit the Pentagon in 2017, but not before getting these three videos declassified and then things took a stranger turn.
Chris Mellon: I tried to help my colleague, Lue Elizondo, elevate the issue in the department and actually get it to the Secretary of Defense.
Christopher Mellon served as deputy assistant secretary of defense for intelligence for Presidents Clinton and George W. Bush and had access to top secret government programs.
Chris Mellon: So it's not us, that's one thing we know.
Bill Whitaker: We know that?
Chris Mellon: I can say that with a very high degree of confidence in part because of the positions I held in the department, and I know the process.
Mellon says he grew concerned nothing was being done about UAPs, so he decided to do something. In 2017, as a private citizen, he surreptitiously acquired the three Navy videos Elizondo had declassified and leaked them to the New York Times.
Chris Mellon: It's bizarre and unfortunate that someone I ke myself has to do something like that to get a national security issue like this on the agenda.
He joined forces with now civilian Lue Elizondo and they started to tell their story to anybody who would listen: to newspapers, the History Channel, to members of Congress.
Chris Mellon: We knew and understood that you had to go to the public, get the public interested to get Congress interested, to then circle back to the Defense Department and get them to start taking a look at it.
And now it is. This past August the Pentagon resurrected AATIP, it's now called the UAP task force; service members now are encouraged to report strange encounters; and the Senate wants answers.
Marco Rubio: Anything that enters an airspace that's not supposed to be there is a threat.
After receiving classified briefings on UAPs, Senator Marco Rubio called for a detailed analysis. This past December, while he was still head of the intelligence committee, he asked the director of national intelligence and the Pentagon to present Congress an unclassified report by next month.
Bill Whitaker: This is a bizarre issue. The Pentagon and other branches of the military have a long history of sort of dismissing this. What makes you think that this time's gonna be different?
Marco Rubio: We're gonna find out when we get that report. You know, there's a stigma on Capitol Hill. I mean, some of my colleagues are very interested in this topic and some kinda, you know, giggle when you bring it up. But I don't think we can allow the stigma to keep us from having an answer to a very fundamental question.
Bill Whitaker: What do you want us to do about this?
Marco Rubio: I want us to take it seriously and have a process to take it seriously. I want us to have a process to analyze the data every time it comes in. That there be a place where this is cataloged and constantly analyzed, until we get some answers. Maybe it has a very simple answer. Maybe it doesn't.
V,

(b) (6)
, Communications
Office of Legislative Affairs and Communications
(b) (6) , DoD Office of Inspector General
O: (b) (6)
(b) (6) @dodig.mil
Connect with us @dod_ig and LinkedIn at DoD Inspector General
http://www.dodig.mil/Mailing-Lists/

From	'(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>, "Stebbins, Steven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>
Cc	'(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Subject	Read out from this morning's Senior Military Assistant's meeting
Date	Mon, 17 May 2021 18:34:14 +0000
Message-Id	<ab0201089ddc4bb9a5f296dc9ad24edf@DODIG.MIL>

Gentlemen,

(b) (5), (b) (6)

USAF noted the UAP story on 60 Minutes had generated lots of media inquiries.

(b) (6)

V/R,

(b) (6)
, DoD Office of Inspector General
m: (b) (6)

From	'(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>, "Stebbins, Steven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "Garrison, Marguerite C., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Roark, Michael J., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Stone, Randolph R., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, "Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Subject	FW: [Non-DoD Source] Ex-official who revealed UFO project accuses Pentagon of 'disinformation' campaign
Date	Thu, 27 May 2021 01:18:50 +0000
Message-Id	<ce26da7eafe9404fa29f922ad6734828@DODIG.MIL>

All,
FYSA.
V,
(b) (6)

Sent with BlackBerry Work
(www.blackberry.com)

From: POLITICO Pro Defense <alert@email.politicopro.com<mailto:alert@email.politicopro.com>>
Date: Wednesday, May 26, 2021, 8:10 PM
To: (b) (6) , OIG DoD <(b) (6) @DODIG.MIL<mailto(b) (6) @DODIG.MIL>>
Subject: [Non-DoD Source] Ex-official who revealed UFO project accuses Pentagon of 'disinformation' campaign

[POLITICO Pro]

Ex-official who revealed UFO project accuses Pentagon of 'disinformation' campaign
By Bryan Bender | 05/26/2021 08:09 PM EDT
[https://static.politico.com/1f/c5/48842823467bbf314c5da5ea8deb/ap20212722614532-1.jpg] A day after Lue Elizondo filed his complaint, the agency's inspector general announced a probe into Pentagon “actions” on UFOs. | Charles Dharapak, File/AP
The former Pentagon official who went public about reports of UFOs has filed a complaint with the agency’s inspector general claiming a coordinated campaign to discredit him for speaking out — including accusing a top official of threatening to tell people he was "crazy," according to documents reviewed by POLITICO.
Lue Elizondo, a career counterintelligence specialist who was assigned in 2008 to work for a Pentagon program that investigated reports of "unmanned aerial phenomenon," filed the 64-page complaint to the independent watchdog on May 3 and has met several times with investigators, according to his legal team.
The claim that the government is trying to discredit him comes weeks before the director of national intelligence and the Pentagon are expected to deliver an unclassified report to Congress about UFOs and the government’s strategy for investigating such encounters. The report is expected to include a detailed accounting of the agencies, personnel and surveillance systems that gather and analyze the data.
“What he is saying is there are certain individuals in the Defense Department who in fact were attacking him and lying about him publicly, using the color of authority of their offices to disparage him and discredit him and were interfering in his ability to seek and obtain gainful employment out in the world,” said Daniel Sheehan, Elizondo’s attorney. “And also threatening his security clearance.”

Sheehan, a public interest lawyer and activist, has a long history <https://christicinstitute.org/docs/DanielSheehan_CV.pdf?source=email> of taking on the federal government on behalf of high-profile clients, including defending the New York Times in the Pentagon Papers case as well as one of the Watergate burglars. He is also widely viewed as a provocateur who has an abiding interest in UFOs and has spoken publicly<https://www.amazon.com/Close-Encounters-Fifth-Kind-Contact/dp/B086D4D3V6?source=email> about alien visitations. He also served as counsel for the Disclosure Project, led by ufologist Steven Greer, that has sought to force more government transparency on UFOs.

When asked for comment, Elizondo referred questions to Sheehan.

Sheehan maintains the goal of Elizondo's IG complaint is much bigger than clearing his name: He wants to compel the Pentagon to clear up all the ambiguity about what it knows about UFOs.

"Nobody seemed to be taking this thing seriously," Sheehan said of Elizondo's concerns when he left the Pentagon in 2017. "The different units and different groups that are responsible for responding to this particular phenomenon … they're not briefing each other on this."

"The old dodge," Sheehan says, "is 'oh well, the real problem was that one shop wasn't communicating with the other shop.' That's the classic bureaucratic dodge. I'm trying to get the Defense Department to clarify for the public and media what exactly is the cartography inside the Defense Department for dealing with this particular phenomenon."

A spokesperson for the Defense Department IG's office declined to comment on the status of Elizondo's complaint. "I cannot speculate or del berate about complaints that our office may have received," said Dwrena Allen. "I certainly cannot confirm or deny the existence of an investigation to the same."

But a day after Elizondo filed his complaint, the IG announced a probe <https://www.politico.com/news/2021/05/04/pentagon-inspector-general-military-ufo-485356?source=email> into Pentagon "actions" on UFOs, which is being undertaken by the assistant inspector general for evaluations on space, intelligence, engineering and oversight.

"We may revise the objective as the evaluation proceeds, and we will consider suggestions from management for additional or revised objectives," stated the IG's memo announcing that probe.

It remains unclear whether Elizondo's claims will be found to merit an official investigation, but his legal team says he is scheduled to meet again with investigators from the IG next month.

Elizondo has become a minor celebrity since he retired from the Pentagon in October 2017 and went public about the Advanced Aerial Threat Identification Program, or AATIP, a secret Pentagon effort that was initiated in 2008 by then-Sen. Harry Reid. POLITICO and the New York Times revealed the existence of the office <https://www.politico.com/magazine/story/2017/12/16/pentagon-ufo-search-harry-reid-216111?source=email> and Elizondo's role in it in December 2017.

Elizondo complained at the time that his Pentagon bosses were failing to take seriously numerous intrusions into military airspace by high-performance aircraft of unknown origin.

"It was during this time I grew increasingly frustrated by the lack of resources and interest by senior leadership," he states in the IG complaint. "UAP reporting to our office was increasing, yet our resources were minimal, and leadership involvement was almost non-existent.

"After increased frustration, " he added, "I became alarmed by the frequency and duration of UAP activity in and around controlled U.S. airspace. The instances seemed more provocative, and during one instance, they came within feet of a U.S. fighter aircraft."

After he retired from government service, Elizondo also shared with the media a trio of Navy videos<https://www.youtube.com/watch?v=rO_M0hLlJ-Q&source=email> he got declassified before he left government service.

He claims he has since endured a coordinated effort to malign his reputation, including Pentagon press statements asserting he had no official role in UFO research, even after his role was officially confirmed. He also alleges a personal vendetta from a Pentagon rival he claims has sought repeatedly to damage his career, including trying to have him investigated for releasing the video after he had been cleared of any wrongdoing.

Elizondo charges "malicious activities, coordinated disinformation, professional misconduct, whistleblower reprisal and explicit threats perpetrated by certain senior-level Pentagon officials," according to the complaint, which includes dozens of supporting documents.

POLITICO is declining to publish the names of the Pentagon officials who are cited in the IG complaint because it is unclear whether they are being investigated.

But Elizondo told the IG he has evidence, in the form of emails, documents and the public record, "which suggests a coordinated effort to obfuscate the truth from the American people while impugning my reputation as a former intelligence officer at the Pentagon."

"These negative actions against me have resulted in great personal and professional challenges to me and my family," he adds in the complaint.

In recounting one episode in the days after he left government service, Elizondo claims a senior official warned him that he would "tell people you are crazy, and it might impact your security clearance."

"I responded … by telling him that he can take any action he thinks is prudently necessary, but that I was not mentally impaired, nor have I ever violated my security oath," Elizondo wrote in the complaint, saying he did not meet with the official again "after our discussion as I feared he would take retribution against me."

The IG complaint also charges that the Pentagon's press operation has engaged in a disinformation campaign to discredit him by suggesting he was lying about his UFO work.

He cites several public statements asserting the department had no record of his involvement in UFOs even after saying that he did<https://theintercept.com/2019/06/01/ufo-unidentified-history-channel-luis-elizondo-pentagon/?source=email> work for AATIP.

"Several internet bloggers were notified ... that I had no duties regarding AATIP and that AATIP did not involve the study of UAPs," Elizondo told the IG. "As a result, the bloggers began to disseminate reporting, accusing me of being a fabricator."

He said when he inquired why the Pentagon had changed its official story about AATIP, he claims one individual directly involved told him he “was not happy with the way this was being handled internally with the Department.” The official also said he “was aware I ran AATIP, but forces within the building were telling him not to admit it," according to Elizondo.

The Pentagon public affairs office declined to comment for this story.

The Defense Department this month publicly acknowledged <http://nickpope.net/wpte19/blog/?source=email> in a statement that the AATIP program was involved in UFO research, but it has not corrected the record on Elizondo's involvement, he says.

“It goes beyond simple ambiguity,” Sheehan said. “There [are] actual discordant narratives that are going on. They’re professing a substantial amount of confusion.”

Elizondo maintains that the efforts to punish him for coming forward continue. The IG complaint outlines that his release of the three unclassified UFO videos was investigated by the Air Force Office of Special Investigations and "there were no findings of me conducting any kind of Unauthorized Disclosure.”

But he says he was contacted this April by the Defense Counterintelligence and Security Agency advising him to submit to a new interview to maintain his clearance even though it was renewed in January 2021. And he maintains he was told it was about concerns over whether he violated the rules when he made the UFO videos public.

"Despite a previous favorable AFOSI investigation, I am under accusation of releasing the videos in an unauthorized manner," he wrote in the IG complaint.

Elizondo has continued to publicly maintain <https://www.politico.com/news/2021/03/25/ufo-sightings-report-478104?source=email> that he believes the government is covering up what it knows about UFO sightings. And Sheehan also claims Elizondo’s experience within the Pentagon’s bureaucracy signifies a much deeper resistance to coming clean.

He said there is “this extraordinarily bizarre process going on in the heart of the national security state bureaucracy where general officers, secretaries of defense are not being briefed in on something that is transparently within their jurisdiction.”

“That is a profound and fundamental problem that they view as being above their pay grade,” Sheehan added. “They know something is going on, and they don’t dare go there.”

View this article online.<https://subscr ber.politicopro.com/article/2021/05/ex-official-who-revealed-ufo-project-accuses-pentagon-of-disinformation-campaign-2057185?source=email>

You received this POLITICO Pro content because your customized settings include: Military, Defense and Security, National Intelligence, Bryan Bender. You can customize all of your alert criteria on your settings page<https://subscriber.politicopro.com/settings?source=email>.

This email alert has been sent for the exclusive use of POLITICO Pro subscriber, [redacted]@dodig.mil<mailto[redacted]@dodig.mil>. Forwarding or reproducing the alert without the express, written permission of POLITICO Pro is a violation of copyright law and the POLITICO Pro subscription agreement.

Copyright © 2021 by POLITICO LLC. To subscribe to Pro, please go to politicopro.com<https://politicopro.com?source=email>.

This email was sent to [redacted]@dodig.mil<mailto[redacted]@dodig.mil> by:
POLITICO, LLC

1000 Wilson Blvd.
Arlington, VA 22209
USA

From	"(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>, "Roark, Michael J., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Stone, Randolph R., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>
Subject	FW: [Non-DoD Source] Government Finds No Evidence That Aerial Sightings Were Alien Spacecraft
Date	Fri, 4 Jun 2021 00:17:10 +0000
Message-Id	<9bed5c7c2aed44bfb06886db4f5bdf30@DODIG.MIL>

All,
Thought you might be interested in the breaking NY Times article below on UAPs.
According to the article, intelligence officials are reporting that they found no evidence that the aerial phenomena seen by Navy pilots are alien spacecraft. Read more below.
V,
(b) (6)

Sent with BlackBerry Work
(www.blackberry.com)

From: (b) (6) <(b) (6) <mailto (b) (6) >>
Date: Thursday, Jun 03, 2021, 8:11 PM
To: (b) (6) ., OIG DoD <(b) (6) @DODIG.MIL<mailto (b) (6) @DODIG.MIL>>
Subject: [Non-DoD Source] Government Finds No Evidence That Aerial Sightings Were Alien Spacecraft

WASHINGTON — American intelligence officials have found no evidence that aerial phenomena witnessed by Navy pilots in recent years are alien spacecraft, but they still cannot explain the unusual movements that have mystified scientists and the military, according to senior administration officials briefed on the findings of a highly anticipated government report.

The report determines that the vast majority of more than 120 incidents over the past two decades did not originate from any American military or other advanced U.S. government technology, the officials said. That determination would appear to eliminate the possibility that Navy pilots who reported seeing unexplained aircraft might have encountered programs the government meant to keep secret.

But that is about the only conclusive finding in the classified intelligence report, the officials said. And while a forthcoming unclassified version, expected to be released to Congress by June 25, will present few other firm conclusions, senior officials briefed on the intelligence conceded that the very ambiguity of the findings meant the government could not definitively rule out theories that the phenomenon observed by military pilots might be alien spacecraft.

Americans' long-running fascination with U.F.O.s has intensified in recent weeks in anticipation of the release of the government report, which is expected to be presented to Congress this month. Former President Barack Obama further stoked the interest when he was asked last month about the incidents on "The Late Late Show with James Corden" on CBS.

"What is true, and I'm actually being serious here," Mr. Obama said, "is that there is footage and records of objects in the skies that we don't know exactly what they are."

The report concedes that much about the observed phenomenon remains difficult to explain, including their acceleration, ability to change direction and submerge. One possible explanation — that the phenomena could be weather or other research balloons — does not hold up in all cases, the officials said, because of changes in wind speed at the times of some of the interactions.

The final report will also contain a classified annex, the officials said. While that annex will not contain any evidence concluding that the phenomenon are alien spacecraft, the officials acknowledged that the fact that it would remain off limits to the public was likely to continue to fuel speculation that the government had secret data about alien visitations to Earth.
Many of the more than 120 incidents examined in the report are from Navy personnel, officials said. The report also examined incidents involving foreign militaries over the last two decades. Intelligence officials believe at l east some of the aerial phenomena could be experimental technology from a rival power, most likely Russia or China.
One senior official briefed on the intelligence said without hesitation that U.S. officials knew it was not American technology. He said there was worry among intelligence and military officials that China or Russia could be e xperimenting with hypersonic technology.

He and other officials spoke on grounds of anonymity because they were not authorized to speak publicly about the about the classified findings in the report.

Russia has been investing heavily in hypersonics, <https://www.nytimes.com/2019/12/27/us/politics/russia-hypersonic-weapon.html> believing the technology offers the ability to evade American missile-defense technology. China has also developed hypersonic weaponry, and included it in military parades. If the phenomenon were Chinese or Russian aircraft, officials said it would suggest the two powers' hypersonic research has far outpaced American military development.

Navy pilots were often unsettled by the sightings. In one encounter, strange objects — one of them l ke a spinning top moving against the wind — appeared almost <https://www.nytimes.com/2019/05/26/us/politics/ufo-sightings-navy-pilots.html> daily from the summer of 2014 to March 2015, high in the skies over the East Coast. Navy pilots reported to their superiors that the objects had no visible engine or infrared exhaust plumes, but that they could reach 30,000 feet and hypersonic speeds.
Lt. Ryan Graves, an F/A-18 Super Hornet pilot who was with the Navy for 10 years, told The New York Times in an interview that "these things would be out there all day." With the speeds he and other pilots observed, he said, "12 hours in the air is 11 hours longer than we'd expect."
In late 2014, a Super Hornet pilot had a near collision with one of the objects, and an official mishap report was filed. Some of the incidents were videotaped, including one taken by a plane's camera in early 2015 that shows an object zooming over the ocean waves as pilots question what they are watching.
The Defense Department has been <https://www.nytimes.com/2017/12/16/us/politics/pentagon-program-ufo-harry-reid.html> collecting such reports for more than 13 years as part of a shadowy, little-known Advanced Aerospace Threat Identification Program within the Pentagon. The program analyzed radar data, video footage and accounts provided by the Navy pilots and senior officers.
The program began in 2007 and was largely funded at the request of Harry Reid, the Nevada Democrat who was the Senate majority leader at the time. It was officially shut down in 2012 when the money dried up, according to the Pentagon. But after the publication of a New York Times article in 2017 about the program and criticism from program officials that the government was not forthcoming about reports about aerial phenomena, the Pentagon restarted the program last summer as the Unidentified Aerial Phenomena Task Force.

The task force's mission was to "detect, analyze and catalog" sightings of strange objects in the sky that could pose a threat to national security. But government officials said they also wanted to remove the stigma for servi ce members who report U.F.O sightings in the hope that more would be encouraged to speak up if they saw something. The goal, officials said, is to give authorities a better idea of what might be out there.

Last year, President Donald J. Trump's budget included a provision<https://www.nytimes.com/2021/06/03/us/ufos-report.html>inserted by lawmakers that the secretary of defense and director of national intelligence submit an unclassified report on what the government knows about U.F.O.s. That report is the one to be released this month.
Officials briefed on the report said it also examined video that shows a whitish oval object<https://www.nytimes.com/2017/12/16/us/politics/unidentified-flying-object-navy.html> described as a giant Tic Tac, about the size of a commercial plane, encountered by two Navy fighter jets off the coast of San Diego in 2004.

In that incident, the pilots reported an interaction with the craft, which lasted for several minutes. At one point, the object peeled away, one of the pilots, Cmdr. David Fravor, said in an interview later with The Times. “It accelerated like nothing I’ve ever seen,” he said.
The report studies that incident, including the video that accompanied the interaction. The provenance of the object is still unknown, the officials said.

Sent from my iPad

From	"(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>
Cc	"(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, "(b) (6)., OIG DoD" <(b) (6) @DODIG.MIL>
Subject	RE: June Newsletter Template_2021
Date	Fri, 4 Jun 2021 15:57:55 +0000
Message-Id	<0056ffdcbf2f49f99a9914646a857447@DODIG.MIL>

Good Morning Sir,
Attached is the updated June Newsletter for your review.
Pending your review and approval, OLAC will finalize and publish to the external website and OIGnet not later than Friday, June 7.

Very Respectfully,
(b) (6)
Office of Legislative Affairs and Communications
DoD Office of Inspector General
O: (b) (6)
C: (b) (6)
(b) (6) @dodig.mil
Connect with us @dod_ig and LinkedIn at DoD Inspector General
http://www.dodig.mil/Mailing-Lists/

From: (b) (6)., OIG DoD
Sent: Friday, June 4, 2021 10:59 AM
To: O'Donnell, Sean W., HON, OIG DoD <(b) (6) @dodig.mil>
Cc: (b) (6), OIG DoD <(b) (6) @DODIG.MIL>; Zola, Michael C., OIG DoD <(b) (6) @DODIG.MIL>; (b) (6)., OIG DoD <(b) (6) @DODIG.MIL>
Subject: RE: June Newsletter Template_2021
Thank you, Sir.
(b) (5).
Once complete, I will return for your review and approval.

Very Respectfully,
(b) (6)
Office of Legislative Affairs and Communications
DoD Office of Inspector General
O: (b) (6)
C: (b) (6)
(b) (6) @dodig.mil
Connect with us @dod_ig and LinkedIn at DoD Inspector General
http://www.dodig.mil/Mailing-Lists/

From: O'Donnell, Sean W., HON, OIG DoD <(b) (6) @dodig.mil>
Sent: Friday, June 4, 2021 10:56 AM
To: (b) (6) OIG DoD <(b) (6) @DODIG.MIL>
Cc: (b) (6), OIG DoD <(b) (6) @DODIG.MIL>; Zola, Michael C., OIG DoD <(b) (6) @DODIG.MIL>; (b) (6), OIG DoD <(b) (6) @DODIG.MIL>
Subject: Re: June Newsletter Template_2021

(b) (5) [redacted]

(b) (5) [redacted]

From: (b) (6) [redacted]., OIG DoD
Sent: Friday, June 4, 2021 10:54:43 AM
To: O'Donnell, Sean W., HON, OIG DoD
Cc: (b) (6) [redacted], OIG DoD; Zola, Michael C., OIG DoD; (b) (6) [redacted], OIG DoD
Subject: RE: June Newsletter Template_2021
Good Morning Mr. O'Donnell,
Apologies for the delay, (b) (6) [redacted] is out today and I am covering Communications.
(b) (5) [redacted].

Very Respectfully,
(b) (6) [redacted]
Office of Legislative Affairs and Communications
DoD Office of Inspector General
O: (b) (6) [redacted]
C: (b) (6) [redacted]
(b) (6) [redacted]@dodig.mil
Connect with us @dod_ig and LinkedIn at DoD Inspector General
http://www.dodig.mil/Mailing-Lists/

From: (b) (6) [redacted], OIG DoD <(b) (6) [redacted]@DODIG.MIL>
Sent: Friday, June 4, 2021 10:09 AM
To: (b) (6) [redacted] OIG DoD <(b) (6) [redacted]@DODIG.MIL>
Subject: FW: June Newsletter Template_2021
FYSA

V/R,
(b) (6) [redacted], DoD Office of Inspector General
m: (b) (6) [redacted]
From: O'Donnell, Sean W., HON, OIG DoD <(b) (6) [redacted]@dodig.mil>
Sent: Friday, June 4, 2021 9:55 AM
To: (b) (6) [redacted]., OIG DoD <(b) (6) [redacted]@DODIG.MIL>
Cc: (b) (6) [redacted], OIG DoD <(b) (6) [redacted]@DODIG.MIL>
Subject: Re: June Newsletter Template_2021

FYI. One question.

From: (b) (6) [redacted]., OIG DoD
Sent: Wednesday, June 2, 2021 10:15:04 AM
To: O'Donnell, Sean W., HON, OIG DoD
Cc: (b) (6) [redacted], OIG DoD
Subject: June Newsletter Template_2021
Good morning, Mr. O'Donnell.
Attached is the June Newsletter for your review.
Pending your review and approval, OLAC will finalize and publish to the external website and OIGnet not later than Friday, June 4.
(b) (6) [redacted] completed his review.

V,
(b) (6)

.....

Attachment Name : June Newsletter Template_2021 v2.docx

UPCOMING REPORTS

Significant reports expected to be issued within the next 30 days include:

Audit of the Reimbursement for Department of Defense Mission Assignments for Coronavirus Disease-2019 Pandemic Response in the U.S. Northern Command Area of Responsibility
This audit determines whether DoD Components (tasked units) requested and received reimbursement of costs incurred for support provided for coronavirus disease-2019 (COVID-19) pandemic response mission assignments in the U.S. Northern Command area of responsibility in accordance with DoD policies.

Audit of the Department of Defense's Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations
This audit determines whether the DoD planned and executed activities to implement memorandums between the DoD and the Department of Homeland Security regarding cybersecurity and cyberspace operations.

Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems
This audit determines whether DoD Components secured additive manufacturing systems to prevent unauthorized changes and ensure the integrity of design data. Additive manufacturing systems are printers and computer workstations used to develop three-dimensional products.

Audit of the Military Departments' Purchases of Aviation Fuel and Non-Fuel Services Using the Aviation Into-Plane Reimbursement Card
This audit determines whether the Military Departments made purchases using the Aviation Into-Plane Reimbursement Card program in accordance with applicable laws and regulations.

Audit of Department of Defense Joint Bases
This audit determines whether Military Service Components met the terms outlined in the joint base memorandums of agreement and whether processes are in place to report and address joint base–related concerns.

Audit of Munitions Storage in the U.S. European Command
This audit determines whether the DoD stored and secured its munitions in the U.S. European Command area of responsibility in accordance with applicable policy. **This report is classified.**

Audit of the Department of Defense's Sea Transportation and Storage of Arms, Ammunition, and Explosives
This audit determines whether the DoD transported arms, ammunition, and explosives by sea in accordance with DoD regulations.

Audit of the Accounting Corrections on the Standard Form 1081
This audit determines whether the DoD properly used the Standard Form 1081, "Voucher and Schedule of Withdrawals and Credits," to correct accounting errors. DoD Components and the Defense Finance and Accounting Service use the Standard Form 1081 to transfer amounts between Fund Balance With Treasury accounts and to make corrections to collections and disbursements.

Physical Security Conditions at U.S. Transportation Command Military Ocean Terminals
This audit determines whether the physical security programs at the U.S. Transportation Command Military Ocean Terminals are protecting shipments of arms, ammunition, and explosives in compliance with DoD, Army, and installation guidance. **This report is classified.**

RECENTLY ISSUED REPORTS OF INTEREST (to view report, if available, please click on title)

Audit of the Department of Defense Coronavirus Aid, Relief, and Economic Security Act Awards to the Defense Industrial Base
This audit determined that the DoD awarded Coronavirus Aid, Relief, and Economic Security Act funding to sustain or increase the Defense Industrial Base in accordance with Federal regulations and Defense Production Act authorities for the six awards that were reviewed. In addition, DoD officials complied with the Federal Acquisition Regulation and the Code of Federal Regulations when awarding the Coronavirus Aid, Relief, and Economic Security Act funding to existing contracts and new technology investment agreements. As a result, the six Defense Industrial Base awards that were reviewed will receive $206.8 million in Coronavirus Aid, Relief, and Economic Security Act funding to help them overcome the financial distress caused by the COVID-19 pandemic and sustain critical national defense.

Audit of the Department of Defense's Compliance in FY 2020 With Improper Payment Reporting Requirements
This audit determined that the DoD did not comply with all of the Payment Integrity Information Act requirements in its FY 2020 reporting of improper payments. The DoD did not publish reliable improper payments estimates for 7 of its 11 programs and missed its annual improper payment reduction target for the Military Health Benefits program because it did not comply with two of the six Payment Integrity Information Act requirements. As a result, DoD leadership and Congress cannot accurately determine whether the DoD has the necessary resources and the appropriate measures in place to reduce its improper payments.

Evaluation of the Air Force Systems Engineering Processes Used in the Development of the Refueling Boom for the KC-46A Tanker
This evaluation determined that the KC-46 Program Office officials did not effectively manage the development of the refueling boom for the KC-46A tanker. For example, KC-46 Program Office officials did not ensure that critical technologies for the refueling boom were demonstrated in a relevant testing environment after Boeing officials presented a system design at the preliminary design review in 2012. Additionally, program officials did not verify full functionality of the KC-46A tanker refueling boom in accordance with the program's Test and Evaluation Master Plan when they performed flight testing of the KC-46A tanker refueling boom with Air Force receiver aircraft. As a result, retrofit of the refueling boom for the delivered KC-46A tankers is not estimated to begin until

January 2024, and will result in additional undetermined costs. This delay also limits the DoD's use of the KC-46A tanker for its intended refueling missions.

Evaluation of the Department of Defense's Handling of Incidents of Sexual Assault Against (or Involving) Midshipmen at the United States Naval Academy
This evaluation determined that United States Naval Academy (USNA) Sexual Assault Prevention and Response personnel provided services to midshipmen-victims of sexual assault, victim support services were available to midshipmen-victims of sexual assault at the USNA, and reports of sexual assault were accurately reported to Congress as required by DoD and Navy policy, and law. The evaluation also determined that Navy Criminal Investigative Service (NCIS) agents responded to and investigated reports of sexual assault in accordance with DoD, Navy, and NCIS policy. Additionally, USNA commanders and decision makers did not retaliate against the three midshipmen-victims who departed the USNA during the scope of the evaluation by separating them from the Navy for reporting their sexual assaults. However, the USNA SAPR personnel did not have a process or system to document "contacts and consults" with midshipmen-victims who chose not to make an official report of sexual assault or a means to document resulting referrals to victim support services.

Quality Control Review of the PricewaterhouseCoopers LLP FY 2019 Single Audit of the Institute for Defense Analyses
This review determined that PricewaterhouseCoopers LLP complied with Generally Accepted Government Auditing Standards and Uniform Guidance requirements from the Code of Federal Regulations when it performed the FY 2019 single audit of the Institute for Defense Analyses.

Summary External Peer Review of the Air Force Audit Agency
This review determined that the system of quality control for the Air Force Audit Agency in effect for the 3-year period ended December 31, 2019, has been suitably designed and complied with to provide the Air Force Audit Agency with reasonable assurance of performing and reporting in conformity in all material respects with applicable professional standards and legal and regulatory requirements. Audit organizations can receive a rating of pass, pass with deficiencies, or fail. The Air Force Audit Agency received a rating of pass for its Special Access Program audits.

DEFENSE CRIMINAL INVESTIGATIVE SERVICE HIGHLIGHTS (to view DOJ press release, if available, please click on title)

Former Air Force Employee Pleads Guilty to Stealing More Than $1.1 Million in Government Funds
On May 14, 2021, in Greenbelt, Maryland, Eddie Ray Johnson, Jr. pleaded guilty to theft of Government property in connection with a scheme to use his Government-issued travel credit card to obtain over $1 million in cash advances. From January 2003 to February 2018, Johnson was a civilian Air Force travel coordinator in the Secretary of the Air Force, Office of Legislative Liaison where he planned congressional travel and reviewed accounting packages submitted by trip escorts. Johnson admitted that he used his Government-issued credit card to obtain more than $1.1 million in cash advances, frequently depositing stolen funds in a non-interest bearing account at a bank branch in the Pentagon. After depositing the stolen funds, Johnson wrote checks to himself for his personal benefit, which he deposited into his personal bank accounts and used for living expenses, a baby grand piano, loan payments for a Harley Davidson motorcycle, and family vacations. In addition, Johnson admitted to

providing cash to his family members. He faces a maximum sentence of 10 years in Federal prison. This was a joint investigation with the Defense Criminal Investigative Service (DCIS), the Air Force Office of Special Investigations, and the Internal Revenue Service Criminal Investigations Division.

Former Chesapeake OB-GYN Sentenced to 59 Years in Prison

On May 18, 2021, in Alexandria, Virginia, a former Chesapeake doctor was sentenced to 59 years in prison after a jury convicted him on 52 counts of health care fraud and other charges stemming from his performance of irreversible hysterectomies, improper sterilizations, and other medically unnecessary procedures over a decade. Javaid Perwaiz, an OB-GYN who practiced in Hampton Roads since the 1980s, executed this scheme to defraud health insurance programs by performing medically unnecessary procedures between 2010 and 2019 that caused approximately $20.8 million in losses to private and Government health care insurers. Perwaiz would falsely tell his patients that they needed surgeries because they had cancer, or to avoid cancer to induce them to agree to the surgeries. Perwaiz also falsified patient records so that he could induce their labor early to ensure he would be reimbursed for the deliveries, violated the 30-day waiting period for elective sterilizations by submitting backdated forms, and billed insurance organizations hundreds of dollars for false diagnostic procedures. This was a joint investigation with DCIS, the Department of Health and Human Services Office of the Inspector General (OIG), and the Federal Bureau of Investigation (FBI).

University of Miami to Pay $22 Million to Settle Claims

On May 10, 2021, the University of Miami (UM) agreed to pay $22 million to resolve allegations that it violated the False Claims Act by ordering medically unnecessary laboratory tests and submitting false claims through its laboratory and hospital based facilities. UM converted multiple physician offices to hospital facilities, and then sought payment at higher rates without providing beneficiaries the required notice, even after being advised by a contractor that its notice practices were deficient. The Government alleged that UM billed Federal health care programs for medically unnecessary laboratory tests for patients who received kidney transplants with a transplant program operated by UM. Each time a patient checked into the program, UM's electronic ordering system triggered a pre-determined set of tests to be run for the patient at UM's laboratory. According to the Government, UM pressured the hospital to purchase pre-transplant laboratory tests from UM at inflated rates in exchange for UM surgeons performing surgeries at the hospital. This was a joint investigation with DCIS, the Department of Health and Human Services OIG, the Office of Personnel Management OIG, the Defense Health Agency, and the Florida Attorney General's Office's Medical Fraud Control Unit.

Jury Convicts Iranian National for Illegally Exporting Military Sensitive Items

On May 7, 2021, a Federal jury in San Antonio, Texas, convicted Mehrdad Ansari, an Iranian citizen and resident of the United Arab Emirates and Germany, for scheming to obtain military sensitive parts for Iran in violation of the Iranian Trade Embargo. These parts had dual-use military and civilian capability and could be used in such systems as nuclear weapons, missile guidance, secure tactical radio communications, offensive electronic warfare, military electronic countermeasures, radar warning, and surveillance systems. According to the evidence presented, Ansari attempted to transship cargo obtained from the U.S. by co-defendants using his companies located in Dubai, United Arab Emirates. From 2007 to 2011, the conspirators obtained or attempted to obtain over 105,000 parts valued at approximately $2.6 million. The conspirators conducted 599 transactions with 63 different U.S. companies in which they obtained or attempted to obtain parts without notification that they were being shipped to Iran, or securing the required Government license to ship them to Iran. Ansari faces up to 40 years in Federal prison. This was a joint

investigation with the DCIS, Homeland Security Investigations, the FBI, and the Department of Commerce Bureau of Industry and Security's Office of Export Enforcement.

(b) (5)

[redacted]

ANNOUNCED PROJECTS (to view the announcement letters, if available, please click on the title)

Audit of the Department of Defense Certification Process for Coronavirus Aid, Relief, and Economic Security Act Section 4003 Loans Provided to Companies Designated as Critical to Maintaining National Security
The objective of this audit is to determine the effectiveness of the DoD's processes to certify and approve businesses critical to maintaining national security for loans under section 4003 of the Coronavirus Aid, Relief, and Economic Security Act.

Audit of the Department of the Navy's Controls Over the Federal Employees' Compensation Act Program
The objective of this audit is to determine whether the Navy effectively managed the Federal Employees' Compensation Act program, including reducing claimant fraud, waste, or abuse.

Evaluation of the Department of Defense's Actions Regarding the Unidentified Aerial Phenomena
The objective of this evaluation is to determine the extent to which the DoD has taken actions regarding Unidentified Aerial Phenomena.

Evaluation of the Department of Defense's Efforts to Address the Climate Resilience of U.S. Military Installations in the Arctic and Sub-Arctic
The objective of this evaluation is to determine the extent to which the DoD has addressed the climate resilience of U.S. military installations in the Arctic and sub-Artic.

Re-Announcement of the Evaluation of Kinetic Targeting Processes in the United States Africa Command Area of Responsibility
The objective of this evaluation is to determine whether U.S. Africa Command and U.S. Special Operations Command established and followed targeting and reporting procedures in the U.S. Africa Command area of responsibility to reduce civilian casualties and collateral damage.

Commented [OSWSOD1]: (b) (5) [redacted]

Formatted: Underline, Highlight
Formatted: Underline, Highlight
Formatted: Highlight
Formatted: Underline, Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight

Audit of Vetting and Continuous Review of International Military Students Enrolled in United States-Based Training Programs and Accompanying Family Members
The objective of this audit is to determine whether the DoD effectively implemented vetting procedures for international military students enrolled in U.S.-based training programs and their accompanying family members with access to DoD installations and facilities in accordance with DoD guidance.

Audit of the Defense Health Agency's Reporting of Improper Payment Estimates for the Military Health Benefits Program
The objective of this audit is to determine whether the Defense Health Agency is accurately identifying and reporting improper payments as required by the Payment Integrity Information Act of 2019.

Joint Audit of Security Controls Over Coast Guard Systems Used and Operated on the Department of Defense Information Network
The objective of this audit is to determine whether the Coast Guard implemented security controls to protect Coast Guard systems used and operated on the DoD Information Network in accordance with applicable cybersecurity requirements.

From	'(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
To	"List .SESLIST" <(b) (6) @dodig.mil>
Cc	"Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6)., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6), OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6), OIG DoD" <(b) (6) @DODIG.MIL>
Subject	Representative André Carson on "Face the Nation," July 4, 2021
Date	Tue, 6 Jul 2021 16:15:26 +0000
Message-Id	<8740d914f9a44c9a8215b75edf3ae2bc@DODIG.MIL>

Good afternoon, all.
As per Michael's comments during the senior staff meeting, please see the transcript and video link below concerning the interview with Rep. Carson on the potential hearing on UFO/UAP sightings.
https://www.cbsnews.com/video/democratic-congressman-andre-carson-wants-hearings-on-ufo-sightings/
Transcript of interview with Representative André Carson of Indiana that aired on Sunday, July 4, 2021, on "Face the Nation."
ED O'KEEFE: In a recently declassified report, US intelligence officials have offered no explanation for dozens of unexplained sightings witnessed by Navy pilots since 2004. Congressman André Carson of Indiana chaired a classified briefing on this report and joins us from Washington. Congressman, happy Independence Day to you. I know you can't share all the details of that classified report. We wish you could. And before we talk about UFOs, I want to ask you about these reports of a new ransomware attack over the weekend that apparently has affected at least dozens of American companies. As a member of the Intelligence Committee, have you learned anything more about it?
REP. ANDRÉ CARSON (D-IN): Well, these attacks obviously have always targeted primarily two pillars of our American foundation, the government and US businesses, and we've seen this debacle with SolarWinds. We've seen it with the Colonial Pipeline. We've been briefed as a committee. We're looking into it. The Biden administration has a very serious plan in terms of pushing back on these attackers. And so along with the startup entities and small businesses and the US government, we're working on encryption. You know, we want a system that is- is protected, but we don't want something that's so impenetrable we can't catch criminals--
###
V,
(b) (6)

From	'(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>, "Stebbins, S teven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OI G DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" < (b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "Roark, Michael J., SES, OIG DoD" <(b) (6) @DODIG.M IL>, "Stone, Randolph R., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @dodig.mil>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Cc	"Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., O IG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>
Subject	Bill text for FY22 Intel Authorization with OIG reporting requirement
Date	Fri, 6 Aug 2021 18:41:38 +0000
Message-Id	<be43d926993a4dea9d5d716793c4751a@DODIG.MIL>

Good afternoon.
The Senate Select Committee on Intelligence (SSCI) has reported its Intelligence Authorization Act for FY 2022 to the Senate and published text for the bill, which includes a reporting requirement for the DoD OIG. Attached is the full bill and an excerpt of section 344, which would require the DoD IG and IC IG to jointly complete a review of the National Security Agency and U.S. Cyber Command and, not later than 180 days after enactment, submit a report and provide a briefing to the intel and defense committees. This requirement is included in bill language and could be revised or removed during conference. OLAC will continue to monitor and provide updates.
Also of interest, sections 321-324 offer provisions related to whistleblowers in the IC, including submitting complaints and information to Congress, definitions and authorities related to information of urgent concern, harmonization of whistleblower protections, and protection against disclosure of WB identity as reprisal.
In addition, section 345 would require IC and DoD elements with data relating to UAPs to make such data available immediately to the UAP Task Force and NASIC. It would also require classified quarterly reports from the DoD on UAP Task Force findings.
Respectfully,

(b) (6)
Office of Legislative Affairs & Communications
Department of Defense Office of Inspector General
4800 Mark Center Drive
Alexandria, VA 22350
#(b) (6)
(b) (6) @dodig.mil

.....

Attachment Name : FY22 IAA Provision with OIG Reporting Requirement.pdf

.....

Attachment Name : S.2610 - IAA for FY22.pdf

SEC. 344. REVIEW OF NATIONAL SECURITY AGENCY AND UNITED STATES CYBER COMMAND.

(a) REVIEW REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community and the Inspector General of the Department of Defense shall jointly complete a review of the National Security Agency and the United States Cyber Command.

(b) ELEMENTS.—The review required by subsection (a) shall include assessment of the following:

(1) Whether resources, authorities, activities, missions, facilities, and personnel are appropriately being delineated and used to conduct the intelligence and cybersecurity missions at the National Security Agency as well as the cyber offense and defense missions of United States Cyber Command.

(2) The extent to which current resource-sharing arrangements between the National Security Agency and United States Cyber Command lead to conflicts of interest in directing intelligence collection in support of United States Cyber Command missions rather than foreign intelligence collection.

(3) The intelligence analysis and production conducted by United States Cyber Command using National Security Agency authorities, with a focus

on analytic integrity and intelligence oversight to ensure proper analysis is informing mission operations.

(c) REPORT AND BRIEF.—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community and the Inspector General of the Department of Defense shall jointly submit to the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) a report and provide such committees a briefing on the findings of the inspectors general with respect to the review completed under subsection (a).

SEC. 345. SUPPORT FOR AND OVERSIGHT OF UNIDENTIFIED AERIAL PHENOMENA TASK FORCE.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' includes:

(A) The congressional intelligence committees.

(B) The Committee on Armed Services of the Senate.

(C) The Committee on Armed Services of the House of Representatives.

From	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6)@dodig.mil>
To	'(b) (6)., OIG DoD" <(b) (6)@DODIG.MIL>, '(b) (6), O IG DoD" <(b) (6)@DODIG.MIL>, '(b) (6), OIG DoD" <(b) (6) @DODIG.MIL>
Subject	Rescheduled QMR #3
Date	Mon, 9 Aug 2021 11:59:51 +0000
Message-Id	<fbf01538ef2540f1a2507309c6133bf1@01AESVC-MBC.dodig.mil>

Attached please find the read ahead slides for next week's QMR 3, Annual Oversight Planning Roundtable.
An overarching list of planned projects and on-going projects is also attached.
Hard copy briefing binders for SES can distr buted provided you will be in the office next week to receive one. If you plan to be around, please let me know and I can drop one off.
If there are any questions related to the briefing or any of the data please let me know.
V/R

(b) (6)
Strategic Planner
DoD Office of the Inspector General
Strategy, Planning, and Performance
Office: (b) (6)
Email: (b) (6)@dodig.mil

QMR #3 rescheduled Aug 12th, 1300-1500 to earlier time 1000-1200.

NOTE: Please remove or decline the Aug 5th QMR #3 meeting invite from Mr. O'Donnell's calendar. Due to Outlook calendar issue, the Aug 5th QMR #3 meeting invite is unable to be cancelled from Mr. O'Donnell's calendar.

Jabber Conf ID: (b) (6), Pass: (b) (6) or Dial-in: (b) (6), ID: (b) (6), Pass: (b) (6)

.....

Attachment Name : FY22 QMR 3 RAH.pdf

.....

Attachment Name : Management Challenge - FY22 Planned and FY21 Ongoing Project Summary.pdf

.....

Attachment Name : Mission Area Focus FYs 20-22.pdf

.....

Attachment Name : FY22 Tech Support Report.pdf

1. Maintaining the Advantage in Strategic Competition

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Readiness and Global Operations (RGO)	329	Audit of Individual Preparedness to Conduct Extreme Cold Weather Operations	The objective of this audit is to determine whether Army and Marine Corps units are equipped to safely operate in extreme cold weather conditions in support of training, exercises, and operations in the Arctic region.	(b) (5) [redacted]			
2022	Audit	Readiness and Global Operations (RGO)	474	Audit of U.S. Indo-Pacific Command's Efforts to Implement the Pacific Deterrence Initiative	To determine whether DoD and the U.S. Indo-Pacific Command (USINDOPACOM) have developed realistic goals and established milestones within the Pacific Defense Initiative (PDI) efforts to defend U.S. interests abroad, deter aggression, and assure allies and partners within the Indo-Pacific region.				
2022	Audit	Readiness and Global Operations (RGO)	645	Audit of Army Oversight of DoD Language Interpretation and Translation Enterprise II Contract	The objective of this audit is to determine whether the Army provided oversight of DoD Language and Interpretation and Translation Enterprise II (DLITE II) contractors in the U.S. Central Command (USCENTCOM) area of responsibility to ensure the contractors fulfilled requirements.				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	55	Evaluation of the Use of Compartmented Geospatial Intelligence Collection for Operation Inherent Resolve	(U) The objective of this evaluation is to evaluate National Geospatial-Intelligence Agency and CENTCOM intelligence collection in support of Operation Inherent Resolve. (classified project).				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	488	(U) Evaluation of the North Warning System	(U) The objective of this evaluation is to determine the extent to which the current North Warning System can support the Joint Force Commander's aerospace warning mission requirements to detect potential airborne threats in the Artic region. (b) (5) [redacted]				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	665	Evaluation of National Geospatial-Intelligence Agency Support to Military Operations	The objective of this evaluation is to determine the extent to which the National Geospatial-Intelligence Agency is collecting, analyzing, and distributing geospatial intelligence in support of military operations.				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	666	Evaluation of the Readiness of U.S. Marine Corps' Pre-Positioned War Reserve Stocks in Support of USINDOPACOM's Operation Plans	The objective of this evaluation is to determine the readiness of the U.S. Marine Corps' (USMC) pre-positioned war reserve stocks (PWRS) in support of USINDOPACOM's OPLANs.				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	667	Evaluation of the Effectiveness of Security Force Assistance Brigades	The purpose of this evaluation is to determine the extent to which the Security Force Assistance Brigades (SFAB) are meeting the Geographic Combatant Commands security force assistance (SFA) requirements and improving U.S. Army Brigade Combat Team (BCT) readiness.				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	669	Evaluation of Security Controls at Sea Ports in the U.S. European Command Area of Responsibility	The objective of this evaluation is to determine the extent to which DoD implemented security controls for multi-modal cargo at selected sea ports of debarkation (SPOD) in the U.S. European Command (USEUCOM) area of responsibility (AOR), in accordance with the Defense Transportation Regulation.				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	709	Evaluation of Governance and Protection of Department of Defense Research and Development of Emergent Technology	The objective of this evaluation is to determine the extent to which the Office of the Under Secretary of Defense for Research and Engineering (OUSD[R&E]) has monitored and mitigated risks when developing new technologies with partners in industry and academia to ensure confidentiality, security, and protection of intellectual property and mission priorities from R&D to implementation.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	303	Evaluation of a Classified NGA Program	Proposal is Classified				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	486	Evaluation of Intelligence Support, Communication, and Information Sharing Across the Hypersonic Community on Adversary Hypersonic Weapon Systems	The objective of this evaluation is to determine whether the Defense Intelligence Enterprise is providing effective unity of effort in coordinating, communicating, and sharing intelligence on adversary hypersonic weapons.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	591	Evaluation of the Technology Readiness of the B-21 Raider Long Range Strike Bomber	The objective of this evaluation is to determine the extent to which the critical technologies used on the Air Force's B-21 Raider Long Range Strike Bomber are mature enough to support the B-21 program's acquisition timeline. (b) (5) [redacted]				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	664	Evaluation of Service Capabilities to Counter Unmanned Aircraft Systems	(U) Classified Objective.(U) Unclassified Summary of Objective: The objective of this evaluation is to determine the extent to which the Services have implemented intelligence support, and techniques, tactics and procedures (TTPs), necessary to employ counter-Unmanned Aircraft Systems (C-UAS) systems.(~~CUI~~) (b) (5) [redacted]				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	691	Evaluation of the Office of Special Investigations Counterintelligence Response to Espionage and Criminal Threats Posed by the People's Republic of China	The purpose of this evaluation is to determine the extent to which OSI's counterintelligence operations in response to Chinese cyber espionage and criminal activities are conducted in accordance with DoD, Service, and OSI policy.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	692	Evaluation of the Exploitation of Foreign Source Materiels Obtained by the DoD	The objective of this evaluation is to identify adversarial foreign materiels exploited (FME) by the DoD and the Intelligence Community (IC) and to determine whether the DoD and IC exploited and disseminated the materiels in accordance with the DoD and IC policies and requirements.				

1. Maintaining the Advantage in Strategic Competition

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	693	Evaluation of the DoD Military Working Dog (MWD) Program	The objective of this evaluation is to determine the extent to which the Air Force, as the executive agency for the DoD MWD program, is complying with DoD and Service policy with regards to MWD requisition, training, utilization, performance standards, and validation testing. (b) (5) [redacted]	(b) (5) [redacted]			
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	543	Audit of the Defense Ordnance Technology Consortium (DOTC) Award Process	We are conducting this audit in response to allegations made to the Defense Hotline. The objective of the audit is to determine whether Army contractingpersonnel competed and awarded Other Transaction (OT) prototype projects for the Defense Ordnance Technology Consortium (DOTC) in accordancewith laws and regulations. (b) (5) [redacted]				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	544	(b) (5) [redacted]	(b) (5) [redacted]				
2021	Audit	Cyberspace Operations (CSO)	80	Audit of the Protection of Military Research Information and Technologies Developed by DoD Academic and Research Partners	The objective of this audit is to determine whether institutions that conduct military research and develop technologies for the DoD have effective security controls inplace to protect DoD information stored on their networks from insider and external cyber threats.				
2021	Audit	Cyberspace Operations (CSO)	478	Audit of the Defense Digital Service Support of DoD Programs and Operations	The objective of this audit is to determine whether the Defense Digital Service(DDS) has achieved its intended outcomes to secure the digital environment in accordance with the DoD Digital Modernization Strategy.				
2021	Audit	Readiness and Global Operations (RGO)	452	Followup Audit of Army Oversight of Logistics Civil Augmentation Program V Government-Furnished Property in Afghanistan	The objective of this followup audit is to determine whether the Army implemented the recommendations identified in Report No. DODIG'2018'040, œArmy Oversight of Logistics Civil Augmentation Program Government-Furnished Property in Afghanistan,Ɖ December 11, 2017, to improve the accountability of Government-Furnished Property.				
2021	Audit	Readiness and Global Operations (RGO)	454	Audit of Training Ranges Supporting Units in the U.S. European Command	The objective of this audit is to determine whether training ranges have the capability and capacity to support combat readiness for units assigned to the U.S. European Command (USEUCOM). (b) (5) [redacted]				
2021	Audit	Readiness and Global Operations (RGO)	467	Audit of Vetting of International Military Students Enrolled in United States-Based Training Programs and Accompanying Family Members	The objective of this audit is to determine the extent to which the DoD implemented vetting procedures for international military students enrolled in U.S.-based training programs and their accompanying family members with access to DoD installations and facilities.				
2021	Audit	Readiness and Global Operations (RGO)	551	Audit of the DoD Counter-Islamic State of Iraq and Syria Train and Equip Fund Stipends to the Vetted Syrian Opposition	The objective of this audit is to determine if the DoD assessed whether Vetted Syrian Opposition (VSO) groups met DoD requirements prior to the DoD providing stipends from the Counter-Islamic State of Iraq and Syria Train and Equip Fund for Syria (CTEF-S) to the VSOs. We will also determine whether the DoD established internal controls to ensure the stipend payments were accurately distributed to VSO groups.				
2021	Audit	Readiness and Global Operations (RGO)	579	Audit of Army Accountability of Government-Furnished Property Under Base Operations Contracts in Kuwait	This audit will determine whether the Army effectively accounted for Government-Furnished Property provided to the base operations support and security services contractor in Kuwait.				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	547	Evaluation of DoD Efforts to Develop and Implement Policy and Procedures Addressing Ideological Extremism within the U.S. Armed Forces	The Objective of this evaluation is to determine the extent to which the DoD and the Services have implemented policy and procedures to prohibit active advocacy and active participation related to supremacist, extremist, or criminal gang doctrine, ideology, or causes, by active-duty military personnel, as required by Department of Defense Instruction 1325.06.				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	548	Evaluation of U.S. Central Command and U.S. Special Operations Command Implementation of DoD's Law of War Program	The objective of this evaluation is to determine the extent to which USCENTCOM and USSOCOM developed and implemented programs in accordance with DoD Law of War requirements in order to reduce potential law of war violations when conducting operations. (b) (5) [redacted]				

1. Maintaining the Advantage in Strategic Competition

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	513	Evaluation of the Department of Defense's Transition from a Trusted Foundry Model to a Zero-Trust Model for Procuring Microelectronics	The objective of this evaluation is to determine whether the DoD has plans and procedures in place to manage and mitigate risks as it transitions from a trusted foundry model to a zero‘trust model for procuring microelectronics.	(b) (5)			
2020	Audit	Readiness and Global Operations (RGO)	402	Audit of U.S. Transportation Command Cargo Scheduling Effectiveness	The objective of this audit is to determine whether DoD military components requested timely airlift and sealift cargo movements through U S. Transportation Command (USTRANSCOM) in accordance with DoD guidance.				
2020	Evaluations	Program, COCOM, and OCO Operations (PCOO)	39	(U) Evaluation of Kinetic Targeting Processes in the USAFRICOM Area of Responsibility	The objective of this evaluation is to determine whether USAFRICOM and USSOCOM developed, implemented, and followed targeting procedures; and whether USAFRICOM established and followed requirements and procedures to report CIVCAS in the USAFRICOM area of responsibility.				
2020	Evaluations	Space, Intelligence, and Oversight (SIO)	245	Evaluation of the Foreign Influence in DoD Research and Development	The objective of this evaluation is to determine whether the Office of the Under Secretary of Defense for Research and Engineering (OUSD[R&E]) is monitoring and mitigating foreign influence into the DoD's Research and Development Programs.				

2. Assuring Space Dominance, Nuclear Deterrence, and Ballistic Missile Defense

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Readiness and Global Operations (RGO)	640	Audit of the National Defense Space Architecture Interoperability with DoD Programs of Record	The objective of this audit is to determine the extent to which the National Defense Space Architecture (NDSA) will be interoperable with DoD programs of record that rely on satellite communications to achieve mission requirements.	(b) (5) [redacted]			
2022	Audit	Readiness and Global Operations (RGO)	644	Audit of U.S. European Command's Missile Defense Capabilities	The objective of this audit is to determine whether U.S. European Command has effectively assessed and mitigated Ballistic Missile Defense risks in its area of operations.				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	317	Evaluation of U.S. Central Command's Defense of Critical Assets Within its Area of Responsibility Against Missiles and Unmanned Aircraft Systems	The objective of this evaluation is to determine the extent to which U.S. Central Command can defend critical assets within its area of responsibility against missile and unmanned aircraft system threats.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	480	Evaluation of the Space Fence Space Situational Awareness System	The objective of this evaluation is to determine whether the Space Fence system's current operational capabilities are aligned to the original requirements for the system, and determine the operational impact of not funding a second radar site for the system.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	687	Evaluation of the DoD's Efforts to Modernize the U.S. Nuclear Command, Control, and Communication System	The objective of this evaluation is to determine the extent to which the DoD has developed and implemented a strategy for modernizing the U.S. Nuclear Command, Control, and Communications (NC3) System.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	696	Evaluation of the Department of Defense's Laser Interferometry Upgrades and Compliance with DoD Policy Requirements for Mitigating Supply Chain Risks and Foreign Influence	(U//~~CUI~~) The objective of this evaluation is to determine extent to which the DoD's laser interferometry upgrades improve United States intelligence, surveillance, and reconnaissance (ISR) capabilities for monitoring satellites and whether the upgrades follow DoD policy requirements for mitigating supply chain risks and foreign influence. (U) (b) (5) [redacted]				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	698	Evaluation of the Nuclear Certification of the Long Range Standoff Missile (LRSO)	The objective of this evaluation is to determine the extent to which the Air Force has developed a plan to nuclear certify the .ong-Range Standoff (LRSO) cruise missile.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	701	Evaluation of Sustaining Engineering Actions for the Minuteman III Missile Program	The objective of this evaluation is to determine the extent to which the Air Force has implemented sustaining engineering actions to maintain functionality of the legacy Minuteman III Intercontinental Ballistic Missile program (Minuteman III) until full deployment of the Ground-Based Strategic Deterrent (GBSD), (b) (5) [redacted]				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	703	Evaluation of Sustaining Engineering Actions for the Air Force's Upgraded Early Warning Radar System	The objective of this evaluation is to determine the extent to which the U.S. Air Force has implemented sustaining engineering actions to ensure that the Upgraded Early Warning Radar (UEWR) system is capable, reliable, and available to meet mission requirements while managing risks. (b) (5) [redacted]				
2021	Audit	Readiness and Global Operations (RGO)	476	Audit of DoD Maintenance of Space Launch Equipment and Facilities	The objective of this audit is to determine the extent to which DoD maintained launch facilities to meet anticipated launch requirements and its ability to increase launches.				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	479	Evaluation of the DoD's Strategy to Test Space-Based Systems in Contested Space Environments	The objective of this evaluation is to determine the extent to which the DoD has developed and implemented a strategy for an integrated test program to validate the survivability of space'based systems in a contested space environment.				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	563	Evaluation of Aircraft High-altitude Electromagnetic Pulse (HEMP) Life Cycle Testing and Test Facility Infrastructure	The objective of this evaluation is to determine the extent to which DoD Program Managers for mission critical aircraft are planning and conducting high-altitude electromagnetic pulse (HEMP) life cycle testing in accordance with DoD Instruction 3150.09, "The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy," April 8, 2015. (b) (5) [redacted]				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	572	Evaluation of the Air Force Selection Process for the Permanent Location of the U S. Space Command Headquarters	The objective of this evaluation is to review the basis for selecting Huntsville, Alabama, as the preferred permanent location of the U.S. Space Command (USSPACECOM) headquarters. (b) (5) [redacted]				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	611	Evaluation of the Notification Procedures that the DoD Has in Place for the Presidential Emergency Satchel	The objective of this evaluation is to determine the extent that DoD processes and procedures are in place and adequate to alert DOD officials in the event that the Presidential Emergency Satchel is lost, stolen, or compromised. (b) (5) [redacted]				

3. Building Resiliency to Environmental Stresses

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	393	Audit of Environmental Threats to Navy Shipyards	The objective of this audit is to determine whether Navy officials appropriately planned for environmental threats to naval shipyards in accordance with Federal and DoD policies.	(b) (5) [redacted]			
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	636	Audit of DoD Oversight of Energy Contracts	The objective of this audit is to determine whether DoD contracting officials assigned qualified contracting personnel to perform oversight of energy contracts in accordance with Federal and DoD policies				
2022	Audit	Readiness and Global Operations (RGO)	649	Audit of Energy Resilience in Emergency Preparedness Plans	The objective of this audit is to determine whether installation officials tested, updated, and practiced the energy resilience section of their installation emergency preparedness plans and modified the plans as appropriate.				
2022	Audit	Readiness and Global Operations (RGO)	650	Audit of Infrastructure Resiliency at Military Installations in Southern California to Mitigate the Effects of Natural Disasters	The objective of this audit is to determine whether military installations in southern California implemented infrastructure improvements to mitigate potential damage caused by natural disasters.				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	569	Audit of DoD Implementation of the DoD Coronavirus Disease 2019 Vaccine Distribution Plan	The objective of this audit is to determine whether DoD officials effectively distributed and administered COVID-19 vaccines to DoD's workforce in accordance with DoD guidance.				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	612	Audit of the DoD Approval Process for Companies Designated as Critical to Maintaining National Security to Obtain Coronavirus Aid, Relief, and Economic Security Act Section	The objective of this audit is to determine the effectiveness of the processes to certify and approve businesses critical to maintaining national security for loans under Section 4003 of the Cororavirus Aid, Relief, and Economic Security Act.				
2021	Audit	Cyberspace Operations (CSO)	625	Audit of Cybersecurity of DoD Mobile Classified Devices	The objective of this audit is to determine to what extent the DoD Components' have controls in place to secure, protect, and use classified mobile devices.				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	577	Evaluation of the Department of Defense's Efforts to Address the Climate Resilience of U.S. Military Installations in the Arctic and Sub-Arctic	The objective of this evaluation is to determine the extent to which the DoD has addressed the climate resilience of U.S. military installations in the Arctic and sub-Artic.				
2018	Evaluations	SPO	319	(b) (5) [redacted]	(b) (5) [redacted]				

4. Improving DoD Cyberspace Operations and Securing its Systems, Networks, and Data

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	61	Audit of Cyber Security of Medical Devices at DoD Medical Treatment Facilities	The objective of this audit is to determine whether the Defense Health Agency implemented effective cyber security controls at DoD medical treatment facilities for Internet protocol connectible medical devices to protect patient health information from unauthorized access and disclosure, in accordance with Federal and DoD regulations.	(b) (5)			
2022	Audit	Cyberspace Operations (CSO)	125	Audit of U.S. Combatant Command Offensive Cyber Operations	The objective of this audit is to determine whether U.S. combatant commands planned and executed offensive cyberspace operations within the scope of their operational plans and contingency plans.				
2022	Audit	Cyberspace Operations (CSO)	181	Audit of DoD's Deconfliction of Cyberspace Operations	The objective of this audit is to determine whether DoD implemented processes to deconflict offensive and defensive cyberspace operations in accordance with policy to prevent compromise of DoD Component and interagency missions and operations.				
2022	Audit	Cyberspace Operations (CSO)	293	Audit of DoD Cybersecurity Requirements for the Foreign Military Sales Program	The objective of this audit is to determine whether the DoD implemented an end-use monitoring program to ensure compliance with cybersecurity requirements for defense articles transferred to foreign governments under the Foreign Military Sales Program.				
2022	Audit	Cyberspace Operations (CSO)	297	Audit of Security Controls Over the DoD Intelligence Community Enclaves	The objective of this audit is to determine whether DoD Intelligence Community agencies implemented security controls and processes at classified enclaves to protect devices, systems, and networks from insider and external cyber threats.				
2022	Audit	Cyberspace Operations (CSO)	510	Audit of Combatant Command Training in a Contested Cyberspace Environment	The objective of this audit is to determine whether combatant commands are conducting training exercises that include the evaluation of the DoD's ability to conduct operations in a contested cyberspace environment.				
2022	Audit	Cyberspace Operations (CSO)	592	FY 2022 Audit of DoD's Compliance With the Federal Information Security Modernization Act of 2014	The objective of this audit is to determine the effectiveness of the DoD's information security policies, procedures, and practices and provide an annual independent evaluation in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).				
2022	Audit	Cyberspace Operations (CSO)	629	Summary of Reports and Testimonies Regarding DoD Cybersecurity from July 1, 2020, Through June 30, 2022	The objective of this audit is to (1) summarize unclassified and classified reports and testimonies regarding DoD cybersecurity that the DoD Office of Inspector General (OIG), the Government Accountability Office (GAO), and other DoD oversight organizations issued between July 1, 2020, and June 30, 2022, concerning DoD cybersecurity; (2) identify cybersecurity trends; and (3) provide a status of open DoD cybersecurity-related recommendations.				
2022	Audit	Cyberspace Operations (CSO)	633	Audit of DoD Software Assurance Countermeasures During Weapon System Acquisitions	The objective of this audit is to determine whether the DoD identified and remediated software vulnerabilities for weapon systems throughout the program's lifecycle.				
2022	Audit	Cyberspace Operations (CSO)	712	Audit of DoD's Actions to Implement Fifth-Generation (5G) Wireless Communications Technologies and Mitigate Associated Cybersecurity Risks	The objective of this audit is to determine the DoD's progress towards implementing Fifth-generation (5G) wireless communications technologies and mitigating associated cybersecurity risks.				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	375	Evaluation of U.S. Special Operations Command Joint Military Information Support Operations Web Operations Center (JMWC)	The objective of this evaluation is to determine whether the U.S. Special Operations Command's Joint Military Information Support Operations Web Operations Center (JMWC) meets the combatant commander's requirements to support the geographic and functional combatant commander's ability to counter adversary messaging and influence in the information environment.				
2021	Audit	Cyberspace Operations (CSO)	406	Audit of DoD's Implementation of the Cybersecurity Information Sharing Act of 2015 (CISA)	The objective of this joint audit is to assess the DoD actions taken in 2019 and 2020 to implement the Cybersecurity Information Sharing Act (CISA) requirements. (b) (5) [redacted] We will submit an unclassified, interagency report to Congress by December 2021.				
2021	Audit	Cyberspace Operations (CSO)	459	Audit of the Implementation of Cybersecurity Controls for U.S Coast Guard Operated DoD Information Network (DoDIN) Systems	The objective of this audit is to determine whether the Coast Guard implemented security controls to protect Coast Guard operated DoD Information Network systems and networks in accordance with DoD cybersecurity requirements.				
2021	Audit	Cyberspace Operations (CSO)	463	FY 2021 Audit of DoD's Compliance With the Federal Information Security Modernization Act of 2014 (FISMA)	The objective of this audit is to determine the effectiveness of the DoD's information security policies, procedures, and practices and provide an annual independent evaluation in accordance with the Federal Information Security Modernization Act of 2014.				
2021	Audit	Cyberspace Operations (CSO)	509	Audit of Management and Oversight of DoD Vulnerability and Mitigation Programs for Protecting the DoD Information Network	The objective of this audit is to determine the extent to which the DoD is managing and overseeing its programs that identify and mitigate vulnerabilities to protect the DoD Information Network from insider and external threats.				
2021	Audit	Cyberspace Operations (CSO)	562	Audit of DoD Actions Taken to Protect the DoD Information Network Resulting From the SolarWinds Orion Compromise	The objective of this audit is to determine the extent of the DoD's actions to identify, respond to, and mitigate any compromise of DoD networks and systems resulting from its use of SolarWinds Orion.				
2020	Audit	Cyberspace Operations (CSO)	238	Audit of DoD's Acquisition and Use of Cloud Computing Services	The objective of this audit is to determine whether DoD Components are acquiring, using, and reporting the use of secure cloud computing in accordance with DoD policy, guidance, and strategy.				

4. Improving DoD Cyberspace Operations and Securing its Systems, Networks, and Data

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2020	Audit	Cyberspace Operations (CSO)	296	Audit of the Collection, Analysis, Dissemination, and Security of Sensitive Information Maintained by the Defense Insider Threat Management and Analysis Center	The objective of this audit is to determine whether the Defense Insider Threat Management and Analysis Center (DITMAC) is integrating Component-level indicators and providing an enterprise-level capability to identify insider threats[redacted]	(b) (5)			
2018	Audit	Cyberspace Operations (CSO)	120	Joint Audit of the DoD's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process	Determine whether DoD Components are maximizing reuse of existing security control test and assessment efforts through the Risk Management Framework.				

5. Protecting the Health and Wellness of Service Members and their Families

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	60	Audit of the Accuracy of Classifying and Reporting of Service Members' Individual Medical Readiness.	The objective of this audit is to determine whether the Military Departments classified and reported service members' individual medical readiness in accordance with DoD policies.	(b) (5)			
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	209	Audit of the Oversight of Contractor Performance on the Military Health System - GENESIS Contract	The objective of our audit is to determine whether Defense Health Agency program and contracting personnel effectively monitored contractor performance during the implementation of Military Health System - GENESIS in accordance with Federal and DoD regulations and guidance.				
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	628	Audit of DoD Medical Care for Victims of Sexual Assault	The objective of our audit is to determine whether the DoD provided adequate medical care to victims of sexual assault at selected medical treatment facilities (MTFs), in accordance with applicable laws and guidance.				
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	630	Audit of DoD use of the Government Purchase Card in support of the Coronavirus Diseaseâ€"2019 Pandemic Response	The objective of this audit is to determine if the DoD's Government Purchase Card cardholders made and documented purchases in support of the Coronavirus Disease"2019 Pandemic in accordance with Federal and DoD policies.				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	704	Evaluation of the Military Health System's Progress in the Transition of Operations to the Defense Health Agency	The objective of this evaluation is to review and evaluate the DHA's progress with transition of the Military Health System's health care, administrative functions, and personnel against congressional, DoD, and DHA milestones. (b) (5)				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	707	Evaluation of the DoD's use of Civilian and Veterans Affairs Partnerships to Meet Medical Provider Readiness Requirements	The objective of this evaluation is to determine the extent to which the DHA and Military Departments have identified and established alternative training and clinical practice sites or partnerships with civilian or VA medical systems to meet Military Department established clinical readiness requirements, in accordance with DoDI 6000.19. (b) (5)				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	483	Evaluation of the Department of Defense's Health, Safety, and Environmental Hazard Identification and Remediation Oversight Reform in Military Housing	The objective of this evaluation is to determine the extent of the Department of Defense's compliance with military housing oversight requirements related to health, safety, and environmental hazard identification and remediation in the FY 2020 National Defense Authorization Act.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	632	Evaluation of the Military Criminal Investigative Organizations' Adult Sexual Assault Investigations	The objective of this evaluation is to determine the extent to which the MCIOs respond to and investigate allegations of sexual assault as required by DoD, Service, and Agency policy.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	660	Evaluation of the Military Criminal Investigative Organization's Confidential Source Programs	(b) (5)				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	688	~~(CUI)~~ Evaluation of Identity Intelligence and Threats to Intelligence Operatives and Operations	Classified				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	689	Evaluation of the Air Force Office of Special Investigations (OSI) Internal Control Systems for Criminal Investigations and Supporting Programs	The purpose of the evaluation is to determine the extent to which the OSI is complying with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Investigations (QSI), the IG Act of 1978, Agency and Service regulations, and internal policies and procedures.				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	540	Audit of TRICARE Ambulance Transportation Reimbursements	The objective of this audit is to determine whether payments to providers for ambulance transports complied with TRICARE reimbursement requirements (b) (5)				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	546	Audit of Substance Abuse (Alcohol) Program Screening and Treatment	The objective of this audit is to determine whether the Defense Health Agency and Military Departments are effectively screening and providing access to care for treatment of alcohol abuse according to DoD guidance.				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	576	Audit of Medical Conditions of Residents in Privatized Military Housing	The objective of this audit is to determine whether, or to what extent, medical conditions of occupants are associated with unsafe or unhealthy privatized military housing units. (b) (5) .				

5. Protecting the Health and Wellness of Service Members and their Families

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2021	Audit	Cyberspace Operations (CSO)	545	Audit of the Reliability of the Department of Defense's Coronavirus Diseaseâ€"2019 Patient Health Data	The objective of this audit is to determine the extent to which the DoD can rely on its coronavirus disease"2019 (COVID-19) patient health data to make public health and clinical care decisions.	(b) (5)			
2021	Audit	Cyberspace Operations (CSO)	558	Audit of the Accuracy and Reliability of the Defense Enrollment Eligibility Reporting System Data	The objective of this audit is to determine the accuracy and reliability of the Defense Enrollment Eligibility Reporting System data that the DoD uses to make personnel and DoD workforce-related decisions.				
2021	Audit	Readiness and Global Operations (RGO)	460	Audit of DoD's Exceptional Family Member Program in Overseas Locations	The objective of this audit is to determine whether the DoD provided military families enrolled in the Exceptional Family Member Program at overseas installations with educational and medical'related services in accordance with their family and individual care plans.				
2021	Audit	Readiness and Global Operations (RGO)	530	Audit of DoD Education Activity Return-to-School Plans	The objective of this audit is to determine whether the DoD Education Activity developed and implemented controls to limit the exposure and spread of COVID'19 at DoD schools.				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	494	Evaluation of the DoD's Implementation of Suicide Prevention Resources for Transitioning Uniformed Service Members	(b) (5) [redacted]				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	626	Evaluation of Combatant Command Communication Challenges with Foreign Nation Partners During the COVID-19 Pandemic	The objective of this evaluation is to determine how U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Indo-Pacific Command, U.S. Southern Command, and their Component Commands mitigated communication challenges with partner nations during the COVID-19 pandemic, documented those mitigation strategies, and considered whether these strategies should be employed in future operations where personal interaction is difficult.				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	662	Follow-Up on Trans-Africa Airlift Support in the U.S. Africa Command (DoDIG-2018-116)	This evaluation will determine whether the actions taken in response to recommendations made in the Trans-Africa Airlift Support in the U.S. Africa Command (DoDIG-2018-116), resolved the underlying challenges related to USAFRICOM training; USAFRICOM's conduct of Services Requirement Review Boards (SRRB); and USTRANSCOMs' policies and procedures for planning and executing service acquisitions.				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	694	Evaluation of Department of Defense Military Medical Treatment Facility Challenges During the Coronavirus Disease-2019 (COVID-19) Pandemic for Fiscal Year 2021	The objective of this evaluation is to determine the challenges, concerns, and needs encountered by medical personnel working at DoD Military Medical Treatment Facilities (MTFs) during the coronavirus disease-2019 (COVID-19) pandemic.				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	702	DoD and Service Identification and Screening of Service Members with Traumatic Brain Injuries (TBI)	The objective of this evaluation is to determine the extent to which the Defense Health Agency (DHA) and Military Service medical departments implemented policies and procedures, and provided oversight, to ensure that Service members who sustained TBIs were identified and screened to determine their appropriate level of care. (b) (5) [redacted]				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	224	Evaluation of DoD Law Enforcement Organizations' Response to Active Shooter Incidents	The objectives of this evaluation are to determine whether the (1) DoD and its law enforcement organizations (LEOs) established active shooter incident policies, plans and training in accordance with DoD and Military Service guidance; (b) (5) [redacted]				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	230	Evaluation of the Military Criminal Investigative Organization (MCIO) Major Procurement Fraud Programs	The objective of this evaluation is to determine whether MCIO MPF investigations complied with DoD, Service, and MCIO policy.				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	557	Systems Review of the U.S. Army Criminal Investigation Division's Internal Control Systems for Criminal Investigations and Supporting Programs	The objective of this evaluation is: (1) To determine the extent to which the USACIDC internal controls and inspections are suitably designed, and operating efficiently and effectively to provide reasonable assurance that its personnel are complying with investigative standards as required by DoD and Service policy in order to produce ensure high quality and timely criminal investigations. (2) To determine the extent to which the USACIDC investigative support programs provide efficient and effective support to criminal investigations. (3) To determine the extent to which the USACIDC personnel respond to, and investigate allegations of, criminal incidents as required by DoD and Service policy.				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	567	Evaluation of the Department of Defense's Reform of Privatized Military Housing Oversight Related to Health, Safety, and Environmental Hazards	The objective of this evaluation is to determine the extent of the Department of Defense's compliance with privatized military housing oversight requirements related to health, safety, and environmental hazards in the FY 2020 National Defense Authorization Act.				
2020	Audit	Acquisition, Contracting, and Sustainment (ACS)	67	Audit of TRICARE Telehealth Services	The objective of this audit is to determine whether the Defense Health Agency (DHA) paid for telehealth services in accordance with Federal and DoD guidance.				
2020	Audit	Readiness and Global Operations (RGO)	148	Audit of Entitlements and Allowances for Deployed Reserve Service Members	The objective of this audit is to determine whether the DoD Reserve Components mobilization process ensures that entitlements and allowances are accurately identified and processed prior to service members' deployment.				
2020	Evaluations	Program, COCOM, and OCO Operations (PCOO)	333	Evaluation of the DoD's Oversight of Privatized Military Housing Contracts	The objective of this evaluation is to determine if the DoD is effectively providing oversight for privatized military housing contracts.				

5. Protecting the Health and Wellness of Service Members and their Families

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2020	Evaluations	Program, COCOM, and OCO Operations (PCOO)	357	Evaluation of Traumatic Brain Injury Screening in the U.S. Central Command Area of Responsibility	The objective of this evaluation is to determine whether USCENTCOM screened, identified, documented, and tracked DoD service members suspected of sustaining a TBI to determine whether a return to duty status for current operations was acceptable or evacuation and additional care was required.	(b) (5) [redacted]			
2020	Evaluations	Space, Intelligence, and Oversight (SIO)	220	Evaluation of the Special Victim Investigation and Prosecution (SVIP) Capability within the Department of Defense	The objective of this evaluation is to determine whether the DoD Special Victim Investigation and Prosecution (SVIP) services DoD and Service organizations provide to victims in response to incidents of covered special victim offenses comply with federal law and Department directives.				
2019	Audit	Cyberspace Operations (CSO)	183	Joint Audit of the Department of Defense and Department of Veterans Affairs' Efforts to Achieve Electronic Health Record Interoperability	The objective of this audit is to determine whether the DoD is developing standards and implementing controls to provide interoperability between the health care systems of the DoD, Department of Veterans Affairs (VA), and external health care providers.				
2019	Audit	Readiness and Global Operations (RGO)	55	Audit of the Department of the Air Force's Actions Taken to Mitigate Physiological Events	(b) (5) [redacted]				

6. Adapting DoD's Acquisition and Contract Management to Mission Requirements

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	72	Audit of the United States Army Corps of Engineers (USACE) Military Construction (MILCON) Projects	The objective of this audit is to determine whether USACE effectively managed MILCON projects in accordance with the Federal and DoD policies to mitigate delays and cost increases.	(b)(5)			
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	168	Audit of the Requirements Development for the MQ-25 Stingray	The objective of this audit is to determine whether the Navy is developing and testing the MQ-25 Stingray performance requirements in accordance with Federal and DoD policies				
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	305	Audit of Department of Defense Commercial Item Part Pricing	The objective of this audit is to determine the effects of changes in commercial item regulations on spare parts prices and the ability of DoD components to sustain weapon systems at fair and reasonable prices.				
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	367	Audit of Department of Defense Technical Data and License Rights to Sustain Systems	The objective of this audit is to determine whether the Military Department officials incorporated technical data and software rights into system and subsystem contract requirements to meet sustainment goals, and evaluated alternative sources to obtaining technical data and software rights in accordance with DoD policies.				
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	470	Audit of Parts Purchased in Support of the F-35 Program	The objective of this audit is to determine whether the DoD is purchasing parts for the F‘35 Program at fair and reasonable prices.				
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	471	Audit of Performance Based Logistics Contracts for Systems, Subsystems, or Components	The objective of this audit is to determine whether DoD Component contracting officials developed and awarded performance based logistics contracts that incentivized contractors to increase performance, increase availability of the weapon system, and reduce overall sustainment cost of systems, subsystems, or components.				
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	472	Audit of the Acquisition of the Air Force Three Dimensional Expeditionary Long-Range Radar	The objective of this audit is to determine whether U.S. Air Force officials are adequately developing and managing the Three Dimensional Expeditionary Long-Range Radar program to meet cost, schedule, and performance requirements in accordance with DoD policies.				
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	642	Audit of the Army's Integrated Visual Augmentation System (IVAS)	The objective of this audit is to determine whether Army officials are producing and fielding Integrated Visual Augmentation System (IVAS) units that meet capability requirements.				
2022	Audit	Cyberspace Operations (CSO)	511	Followup Audit on the DoD's Implementation of Cybersecurity Controls and Incident Response Procedures for Industrial Control Systems Supporting the Defense Critical Infrastructure	The objective of this follow up audit is to determine whether the DoD implemented cybersecurity controls to detect, mitigate, report, and respond to cyber attacks on industrial control systems supporting the Defense Critical Infrastructure in accordance with Federal and DoD guidance.				
2022	Audit	Readiness and Global Operations (RGO)	643	Audit of European Deterrence Initiative (EDI) Military Construction Projects (MILCON)	The objective of this audit is to determine whether DoD Construction Agents assigned to European Defense Initiative projects within U.S. European Command implemented oversight and control mechanisms to ensure military construction projects met cost, schedule, and performance objectives in accordance with law, DoD policy, and contractual obligations.(b)(5) .				
2022	Audit	Readiness and Global Operations (RGO)	652	Followup Audit of the Navy's Oversight and Administration of Base Operating Support Services Contracts in Bahrain	The objective of this followup audit is to determine whether the U.S. Navy implemented the recommendations identified in DoD OIG Report No. DODIG-2018-074, œThe U.S. Navy's Oversight and Administration of the Base Support Contracts in Bahrain,Ÿ February 13, 2018, to improve contract oversight and administration.				
2022	Audit	Readiness and Global Operations (RGO)	655	Summary Audit of Systemic Weaknesses in DoD's Oversight of Government Furnished Property	The objective of this audit is to identify and summarize systemic weaknesses in the DoD's oversight of Government Furnished Property.				
2022	Audit	Readiness and Global Operations (RGO)	659	Audit of Repair and Maintenance Requirements within Weapons Systems Acquisitions Contracts	The objective of this audit is to determine whether excessive costs or reductions in readiness have resulted from contractual requirements or technical limitations for major weapons systems that require equipment to be shipped to designated repairers, as compared to equipment that can be repaired onsite by technically trained service members.				
2022	Evaluations	Program, COCOM, and OCO Operations (PCOO)	695	Evaluation of the Military Sealift Command's Surge Sealift Readiness in a Global Crisis	The objective of this evaluation is to determine the Military Sealift Command's readiness to deploy, operate, and maintain the surge to meet the demands of critical supplies and equipment requirements through contracts with venders during a global crisis.				

6. Adapting DoD's Acquisition and Contract Management to Mission Requirements

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	670	Quality Control Review on Single Audit of Advanced Technology International	The objective of this quality control review (QCR) is to determine whether the auditors performed the single audit of Advanced Technology International in accordance with generally accepted government auditing standards and Federal recuirements for single audits.	(b) (5) [redacted]			
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	676	Quality Control Review on Single Audit of the Geneva Foundation	The objective of this quality control review (QCR) is to determine whether the auditors performed the single audit of the Geneva Foundation in accordance with generally accepted government auditing standards and Federal requirements for single audits.				
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	677	Quality Control Review on Single Audit of the United Service Organization, Inc.	The objective of this quality control review (QCR) is to determine whether the auditors performed the single audit of United Service Organization in accordance with generally accepted government auditing standards and Federal requirements for single audits.				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	370	Audit of Department of Defense Other Transactions and the Use of Non-traditional Contractors	The objective of this audit is to determine whether DoD contracting officials used non-traditional contractors when awarding Other Transactions in accordance with applicable federal laws and DoD policies (b) (5) [redacted]				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	455	Audit on the DoD Components' Award and Administration of Cost-Reimbursement Contracts	The objective of this audit is to determine whether DoD officials awarded and administered cost-reimbursable contracts according to Federal and DoD regulation and guidance. (b) (5) [redacted] .				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	560	Audit of the Office of Net Assessment's Contracting Administration Procedures	The objective of our audit is to determine whether contract administration of the DoD Office of Net Assessments contracts complied with applicable Federal and DoD policies.				
2020	Audit	Acquisition, Contracting, and Sustainment (ACS)	352	Audit of Sole-Source Depot Maintenance Contracts	The audit objective is to determine whether the Military Services negotiated fair and reasonable prices for sole-source depot maintenance contracts performed at contractor facilities.				
2020	Audit	Acquisition, Contracting, and Sustainment (ACS)	462	Audit of DoD Selection of Middle-Tier Acquisition Rapid Prototyping and Rapid Fielding Programs	The objective of this audit is to determine whether DoD Component acquisition officials designated programs for the middle-tier acquisition rapid prototyping or rapid fielding in accordance with DoD guidance.				
2020	Audit	Acquisition, Contracting, and Sustainment (ACS)	531	Audit of Contracts Awarded and Administered by the Defense Media Activity	The objective of this audit is to determine whether Defense Media Activity (DMA) personnel properly awarded and administered contracts in accordance with Federal and DoD regulations and guidance.				
2020	Audit	Acquisition, Contracting, and Sustainment (ACS)	535	Audit of the Defense Logistics Agency Award and Management of Fuel Contracts in Areas of Contingency Operations	(b) (5) [redacted] . The objective of this audit is to determine whether Defense Logistics Agency (DLA) Energy personnel awarded and met requirements for fuel contracts, in areas of contingency operations, as required by Federal and DoD guidance. (b) (5) [redacted]				
2020	Audit	Cyberspace Operations (CSO)	346	Audit of Oversight of the Encore III Information Technology Service Task Orders	The objective of this audit is to determine whether DoD Components administered task orders issued under the Defense Information Systems Agency (DISA) ENCORE III information technology (IT) service contract in accordance with Federal and DoD requirements.				
2019	Audit	Acquisition, Contracting, and Sustainment (ACS)	229	Audit of the DoD Foreign Military Sales Acquisition Process	We will determine whether the DoD managed the acquisition of defense articles and services to meet partner country foreign military sales requirements, and whether the metrics used by the DoD components maximize the results of the acquisition process.				
2019	Audit	Acquisition, Contracting, and Sustainment (ACS)	388	Audit of Transdigm Group, Inc.'s Business Model and Its Affect on DoD Spare Parts Pricing	The objective of this audit is to determine whether TransDigm Group, Inc.'s business model affects DoD's ability to pay fair and reasonable prices for spare parts.				

7. Reinforcing the Domestic Supply Chain and Reducing Dependence on Foreign Sources

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	637	Followup Audit of the Defense Logistics Agency Aviation Product Quality Deficiency Report Processing	The objective of this followup audit is to determine whether Defense Logistics Agency Aviation personnel processed product quality deficiency reports (PQDRs) and identified the root cause for defective spare parts in accordance with DoD guidance and obtained restitution (repair, replacement, or refund) from contractors that provided defective spare parts.	(b) (5)			
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	639	Audit of the Defense Logistics Agency Storage of Program Executive Office Ground Combat Systems Equipment	The objective of the audit is to determine whether Defense Logistics Agency (DLA) officials properly maintained and stored Army Program Executive Office Ground Combat Systems (PEO GCS) equipment in accordance with DoD policies				
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	654	Audit of B-52 Critical Spare Parts Inventory	The objective of this audit is to determine whether the Air Force has an effective sustainment strategy for critical spare parts supporting the B-52 aircraft.				
2022	Audit	Cyberspace Operations (CSO)	711	Audit of the Defense Logistics Agency's Cybersecurity Supply Chain Risk Management	The objective of this audit is to determine whether the Defense Logistics Agency is implementing cybersecurity supply chain risk management practices in accordance with Federal and DoD requirements for DoD products it acquires with information technology hardware and software.				
2022	Audit	Readiness and Global Operations (RGO)	646	Audit of Defense Logistics Agency Storage and Disposal of Hazardous Material	The objective of this audit is to determine to what extent Defense Logistics Agency (DLA) Disposition Services stores and disposes of hazardous material in accordance with DoD requirements.				
2022	Audit	Readiness and Global Operations (RGO)	647	Audit of Test, Measurement, and Diagnostic Equipment Used to Maintain Weapon Systems	The objective of this audit is to determine to what extent DoD repair facilities have test, measurement, and diagnostic equipment (TMDE) available to meet requirements for maintaining weapon systems.				
2022	Audit	Readiness and Global Operations (RGO)	648	(b) (5)	(b) (5) .				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	368	Audit of the Department of Defense's Implementation of Predictive Maintenance Strategies to Support Weapon System Sustainment	The objective of this audit is to determine whether the DoD is tracking, monitoring, and effectively sharing lessons learned regarding impacts of predictive maintenance on weapon system sustainment. (b) (5)				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	449	Audit of the DoD Federal Mall Purchases	The objective of this audit is to determine whether the DoD properly made purchases through Federal Mall in accordance with Federal and DoD policies.				
2021	Audit	Readiness and Global Operations (RGO)	405	Audit of the Tracking, Recovery, and Reuse of Department of Defense-Owned Shipping Containers	The objective of this audit is to determine to what extent the Army, Navy, and Marine Corps complied with DoD requirements to: (1) track, recover, and reuse shipping containers, and (2) include those containers in an accountable property system of record.				
2021	Audit	Readiness and Global Operations (RGO)	439	Audit of the Reuse of Excess Department of Defense Property	The objective of this audit is to determine whether the DoD Components reused excess Defense Logistics Agency (DLA)-managed property to fill existing needs before initiating new procurements for the same items.				
2021	Audit	Readiness and Global Operations (RGO)	537	Audit of Navy and Marine Corps Actions to Address Corrosion on FA-18C-G Aircraft Project Proposal	(b) (5) .				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	498	Evaluation of the DoD's Mitigation of Foreign Suppliers in the Pharmaceutical Supply Chain	The objective of this evaluation is to determine whether the DoD has mitigated the risks of interruptions to the pharmaceutical supply chain, due to DoD's reliance on foreign suppliers.				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	552	Evaluation of U.S. Special Operations Command's Supply Chain Risk Management for the Security, Acquisition, and Delivery of Specialized Equipment	(b) (5) .				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	575	Evaluation of the DoD's Actions to Develop Interoperable Joint Logistics Enterprise Systems and Tools for Demand Forecasting	The objective of this evaluation is to determine the extent to which the DoD developed interoperable Joint Logistics Enterprise systems and tools for forecasting demand for campaign and contingency planning, as required by Federal law and DoD policy.				
2020	Audit	Cyberspace Operations (CSO)	501	Audit of the Development and Use of Security Classification Guides to Protect Department of Defense Information	The objective of this audit is to determine whether DoD Components developed security classification guides in accordance with DoD guidance and used the security classification guides to consistently protect DoD information.				
2020	Audit	Readiness and Global Operations (RGO)	445	Audit of the Department of Defense Management of Depot-Level Reparables (DLRs) for Major-End Items	The objective of this audit is to determine whether the Military Services manage depot-level reparables to meet DoD requirements for maintaining authorized stock levels and to meet program readiness levels.				
2020	Evaluations	Space, Intelligence, and Oversight (SIO)	310	(U) Evaluation of ISR Sensor Supply Chain Lifetime Purchases (Classified Title on SIPR)	(U) The objective of this evaluation is to determine whether DoD lifetime buys mitigate security risks to the intelligence, surveillance, and reconnaissance (ISR) supply chains from foreign ownership, control, and influence over contract suppliers.				
2020	Evaluations	Space, Intelligence, and Oversight (SIO)	312	(U) Evaluation of the National Industrial Security Program Contract Classification System	(U) The objective of this evaluation is to determine whether DoD components are using the National Industrial Security Program (NISP) Contract Classification System (NCCS) in accordance with security guidance from the Under Secretary of Defense (Intelligence) for monitoring contractors' safeguarding of DoD classified information.				

8. Improving DoD Financial Management and Budgeting

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Acquisition, Contracting, and Sustainment (ACS)	653	Audit of the Department of Defense's Internal Controls of Financial Assistance Awards	The objective of this audit is to determine whether the DoD's internal controls prevented recipients from receiving funding to perform the same work under multiple financial assistance awards.	(b) (5)			
2022	Audit	Financial Management and Reporting (FMR)	584	Oversight of the Audit of the FY 2022 Department of the Air Force General Fund Financial Statements	(b) (5) . The objective of the IPA's audit will be to determine whether the FY 2022 Department of the Air Force General Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project will be to provide contract oversight of the IPA's audit of the Department of the Air Force General Fund financial statements for the fiscal years ending September 30, 2022 and September 30, 2021 and to determine whether the IPA complied with applicable auditing standards.				
2022	Audit	Financial Management and Reporting (FMR)	586	Oversight of the Audit of the FY 2022 Department of the Army General Fund Financial Statements	(b) (5) .				
2022	Audit	Financial Management and Reporting (FMR)	587	Oversight of the Audit of the FY 2022 DoD Medicare-Eligible Retiree Health Care Fund Financial Statements	(b) (5) . The objective of the IPA's audit is to determine whether the FY 2022 MERHCF financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the MERHCF financial statements for the fiscal years ending September 30 2022 and September 30, 2021, and to determine whether the IPA complied with applicable auditing standards.				
2022	Audit	Financial Management and Reporting (FMR)	588	Oversight of the Audit of the FY 2022 Defense Health Agency Contract Resource Management Financial Statements	(b) (5) . The objective of the IPA's audit is to determine whether the FY 2022 DHA-CRM financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the DHA-CRM financial statements for the fiscal years ending September 30, 2022 and September 30, 2021, and to determine whether the IPA complied with applicable auditing standards.				
2022	Audit	Financial Management and Reporting (FMR)	589	Oversight of the Audit of the FY 2022 Military Retirement Fund Financial Statements	(b) (5) .				
2022	Audit	Financial Management and Reporting (FMR)	590	Attestation of the Agreed-Upon Procedures for Reviewing the FY 2022 Civilian Payroll Withholding	The objective of this agreed-upon procedures engagement is to assist the Office of Personnel Management in assessing whether retirement, health benefits, and life insurance withholdings and contributions as well as enrollment information submitted via the Semiannual Headcount Report by the Defense Finance and Accounting Service for FY 2022 were reasonable. (b) (5) .				
2022	Audit	Financial Management and Reporting (FMR)	593	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Army's System Supporting the Delivery of Munitions Inventory Management Services	(b) (5) .				

8. Improving DoD Financial Management and Budgeting

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Financial Management and Reporting (FMR)	594	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Defense Enterprise Accounting and Management System	(b) (5) . The objective of the IPA's attestation examination is to issue an opinion on the Air Force's description of DEAMS and support services and the suitability of the design of the controls to achieve the related control objectives stated in the description. The objective of our oversight project is to provide contract oversight of the IPA's attestation examination and determine whether the IPA complied with applicable attestation standards.	(b) (5)			
2022	Audit	Financial Management and Reporting (FMR)	595	Oversight of the Audit of the FY 2022 Department of the Air Force Working Capital Fund Financial Statements	(b) (5) . The objective of the IPA's audit is to determine whether the FY 2022 DAF WCF financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the DAF WCF financial statements for the fiscal years ending September 30, 2022 and September 30, 2021 and to determine whether the IPA complied with applicable auditing standards.				
2022	Audit	Financial Management and Reporting (FMR)	596	Oversight of the Audit of the FY 2022 United States Marine Corps General Fund Financial Statements	(b) (5) . The objective of the IPA's audit is to determine whether the FY 2022 USMC General Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the USMC General Fund Financial Statements for the fiscal year ending September 30, 2022 and September 30, 2021, to determine whether the IPA complied with applicable auditing standards.				
2022	Audit	Financial Management and Reporting (FMR)	597	(b) (5)	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	598	Audit of the Department of Defense's Compliance in Fiscal Year 2022 With Payment Integrity Information Act Requirements	The objective of this audit is to determine whether, in FY 2022, the DoD complied with Public LawNo. 116-117 œPayment Integrity Information Act of 2019,Ø March 2, 2020.				
2022	Audit	Financial Management and Reporting (FMR)	599	Audit of the Reliability of the Improper Payment Estimates Reported for the Army Military Pay Program	The objective of this audit is to determine whether the Defense Finance and Accounting Services (DFAS) accurately identified and reported improper payments for the Army Military Pay program.				
2022	Audit	Financial Management and Reporting (FMR)	600	Oversight of the Audit of the FY 2022 Defense Health Program Financial Statements	(b) (5) . The objective of the IPA firm's audit is to determine whether the FY 2022 DHP financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA firm's audit of the DHP financial statements for the fiscal years ending September 30, 2022 and September 30, 2021 and to determine whether the IPA firm complied with applicable auditing standards.				
2022	Audit	Financial Management and Reporting (FMR)	601	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the General Fund Enterprise Business System	(b) (5) .				
2022	Audit	Financial Management and Reporting (FMR)	602	Oversight of the Audit of the FY 2022 Defense Information Systems Agency General Fund Financial Statements	(b) (5) The objective of the independent accounting firm's audit is to determine whether the FY 2022 Defense Information Systems Agency's General Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the independent accounting firm's audit of the Defense Information Systems Agency's General Fund financial statements for the fiscal years ending September 30, 2022 and September 30, 2021 and to determine whether the independent public accounting firm complied with applicable auditing standards.				
2022	Audit	Financial Management and Reporting (FMR)	603	Oversight of the Audit of the FY 2022 Defense Information Systems Agency Working Capital Fund Financial Statements	(b) (5) . The objective of the independent public accounting firm audit is to determine whether the FY 2022 Defense Information Systems Agency's Working Capital Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the independent public accounting firm's audit of the Defense Information Systems Agency Working Capital Fund financial statements for the fiscal years ending September 30, 2022 and September 30, 2021 and to determine whether the independent public accounting firm complied with applicable auditing standards.				

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Financial Management and Reporting (FMR)	605	Oversight of the Audit of the FY 2022 U.S. Army Corps of Engineers-Civil Works Financial Statements	(b) (5)	(b) (5)			
2022	Audit	Financial Management and Reporting (FMR)	606	Oversight of the Audits of the FY 2022 U.S. Army Corps of Engineers Sub-Allotted Funds Financial Statements	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	607	Oversight of the Audit of the FY 2022 U.S. Transportation Command Working Capital Fund Financial Statements	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	608	Oversight of the Audit of the FY 2022 Department of the Army Working Capital Fund	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	609	Oversight of the FY 22 Department of Navy Working Capital Fund Financial Statement Audits and Examinations	(b) (5) The objective of the IPA's audit will be to determine whether the FY 2022 Department of the Navy Working Capital Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project will be to provide contract oversight of the IPA's audit of the Department of the Navy Working Capital Fund financial statements for the fiscal years ending September 30, 2022 and September 30, 2021 and to determine whether the IPA complied with applicable auditing standards.				
2022	Audit	Financial Management and Reporting (FMR)	613	Oversight of the Audit of the FY 2022 Defense Logistics Agency General Fund Financial Statements.	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	614	Oversight of the Audit of the FY 2022 Defense Logistics Agency Working Capital Fund Financial Statements.	(b) (5)				

8. Improving DoD Financial Management and Budgeting

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Financial Management and Reporting (FMR)	615	Oversight of the Audit of the FY 2022 Defense Logistics Agency National Defense Stockpile Transaction Fund Financial Statements.	(b) (5)	(b) (5)			
2022	Audit	Financial Management and Reporting (FMR)	616	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Defense Agencies Initative	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	618	Audit of the DoD Agency-Wide Basic Financial Statements for the Fiscal Years Ending September 30, 2022, and September 30, 2021	The objective of this audit is to determine whether the DoD Agency-Wide Basic Financial Statements as of September 30, 2022 and 2021, taken as a whole, are presented fairly, in all material respects, and in conformity with accounting principles generally accepted in the United States of America. In addition, we will determine whether these principles are consistently applied.				
2022	Audit	Financial Management and Reporting (FMR)	619	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Wide Area Workflow System	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	620	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Defense Automatic Addressing System	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	621	(b) (5)	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	622	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Defense Property Accountability System	(b) (5)				
2022	Audit	Financial Management and Reporting (FMR)	623	Oversight of the Audit of the FY 2022 United States Special Operations Command (USSOCOM) General Fund Financial Statements	(b) (5) The objective the IPA audit is to determine whether the FY 2022 USSOCOM financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA audit of USSOCOM's financial statements for the fiscal years ending September 30, 2022 and September 30, 2021 and to determine whether the IPA complied with applicable auditing standards.				

8. Improving DoD Financial Management and Budgeting

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Financial Management and Reporting (FMR)	624	Oversight of the FY 22 Department of Navy General Fund Financial Statement Audits and Examinations	(b) (5) [redacted]. The objective of the IPA's audit will be to determine whether the FY 2022 Department of the Navy General Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project will be to provide contract oversight of the IPA's audit of the Department of the Navy General Fund financial statements for the fiscal years ending September 30, 2022 and September 30, 2021 and to determine whether the IPA complied with applicable auditing standards.	(b) (5) [redacted]			
2022	Evaluations	Evaluations Support Center (ESC)	663	External Inspection and Evaluation Peer Review of the Department of Interior Office of the Inspector General	The objective of this external peer review is to determine to what extent the Department of Interior Office (DOI) of the Inspector General (OIG): (1) complied with the covered Council of the Inspector General on Integrity and Efficiency Quality Standards for Inspection and Evaluation (Blue Book standards), and (2) selected project and reports complied with the same covered Blue Book standards and the association internal policies and procedures.	[redacted]			
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	504	Evaluation of Defense Contract Management Agency Preaward Financial Capability Reviews on Prospective DoD Contractors	The objective of this evaluation is to determine the extent to which the Defense Contract Management Agency (DCMA) performed preaward financial capability reviews on prospective DoD contractors in accordance with the requirements of the Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), and DCMA policies and operating procedures. (b) (5) [redacted]	[redacted]			
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	683	External Peer Review of the U.S Special Operations Command Office of Inspector General, Audit Division	The objective of this external peer review (peer review) is to determine whether the quality control program for the U.S. Special Operations Command Office of Inspector General, (USSOCOM OIG) Audit Division, for the period ended December 31, 2021, is designed to provide reasonable assurance that the policies and procedures related to the	[redacted]			
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	684	Oversight of the Naval Audit Service External Peer Review	The objective of this evaluation is to provide oversight of the Air Force Audit Agency's peer review of the Naval Audit Service for the 3-year period ended December 31, 2021.	[redacted]			
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	685	External Peer Review of the Army Internal Review Program	The objective of this external peer review (peer review) is to determine whether the quality control program for the Army Internal Review (Army IR) Program, for the period ended December 31, 2021, It is designed to provide reasonable assurance that the policies and procedures related to the system of quality control are suitably designed, operating effectively, and complied with in practice.	[redacted]			
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	686	External Peer Review of the Defense Logistics Agency Office of Inspector General Audit Organization	The objective of this external peer review (peer review) is to determine whether the quality control program for the Defense Logistics Agency Office of Inspector General (DLA OIG Audit Organization), for the period ended September 30, 2022, is designed to provide reasonable assurance that the policies and procedures related to the system of audit quality are suitably designed, operating effectively, and complied with in practice.	[redacted]			
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	697	Evaluation of DoD Contracting Officers' Use of Quick-Closeout Procedures in Class Deviation Authority 2019-0009 to Close DoD Contracts	The objective of this evaluation is to determine the extent to which DoD contracting officers used the Class Deviation 2019-0009, Contract Quick-Closeout Procedures, in the best interest of the DoD to close DoD contracts.	[redacted]			
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	699	Evaluation of Navy Contracting Officer Actions on Defense Contract Audit Agency Audit Findings and Recommendations	The objective of this evaluation is to determine the extent to which Navy contracting officer actions on Defense Contract Audit Agency (DCAA) audit findings complied with the Federal Acquisition Regulation (FAR), DoD policies, and Navy policies.	[redacted]			
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	564	(b) (5) [redacted]	(b) (5) [redacted]	[redacted]			
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	610	Audit of the U.S. Northern Command Execution of the CARES Act Funding	The objective of the audit is to determine whether U.S. Northern Command officials used Coronavirus Aid, Relief, and Economic Security Act funding to support the coronavirus disease-2019 pandemic response and operations in accordance with applicable Federal laws and DoD policies.	[redacted]			
2021	Audit	Financial Management and Reporting (FMR)	371	Oversight of the Audit of the FY 2021 Department of the Air Force General Fund Financial Statements	(b) (5) [redacted]	[redacted]			

8. Improving DoD Financial Management and Budgeting

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2021	Audit	Financial Management and Reporting (FMR)	386	Oversight of the FY 2021 Department of the Air Force Statement on Standards of Attestation Engagement No. 18 Examination of the Defense Enterprise Accounting and Management System	(b) (5) [redacted]	(b) (5) [redacted]			
2021	Audit	Financial Management and Reporting (FMR)	387	Oversight of the Audit of the FY 2021 Department of the Air Force Working Capital Fund Financial Statements	(b) (5) [redacted]				
2021	Audit	Financial Management and Reporting (FMR)	389	Oversight of the Audit of the FY 2021 Defense Health Program General Fund Basic Financial Statements	(b) (5) [redacted]				
2021	Audit	Financial Management and Reporting (FMR)	390	Attestation of Department of State Funds Transferred to DoD for Human Immunodeficiency Virus / Acquired Immune Deficiency Syndrome Prevention	The objective of the review is to attest as to whether the DoD obligated and used funds transferred from the Departmert of State (DoS) under a memorancum of agreement (MOA) to support efforts to meet human immunodeficiency virus (HIV) and acquired immune deficiency syndrome (AIDS) prevention, care, and treatment goals set forth in the U.S. Leadership Act and the President's Emergency Plan for AIDS Relief (PEPFAR).				
2021	Audit	Financial Management and Reporting (FMR)	391	Oversight of the Audit of the FY 2021 DoD Medicare-Eligible Retiree Health Care Fund Basic Financial Statements	(b) (5) [redacted]				
2021	Audit	Financial Management and Reporting (FMR)	392	Oversight of the Audit of the FY 2021 Defense Health Agency Contract Resource Management Basic Financial Statements	(b) (5) [redacted]				
2021	Audit	Financial Management and Reporting (FMR)	397	Oversight of the Audit of the FY 2021 Department of the Navy Working Capital Fund Financial Statement Audit	(b) (5) [redacted]				
2021	Audit	Financial Management and Reporting (FMR)	398	Oversight of the Audit of the FY 2021 United States Marine Corps General Fund Financial Statements	(b) (5) [redacted]. The objective of the IPA's audit is to determine whether the FY 2021 USMC General Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the USMC General Fund Financial Statements for the fiscal year ending September 30, 2021 and September 30, 2020, to determine whether the IPA complied with applicable auditing standards.				

8. Improving DoD Financial Management and Budgeting

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2021	Audit	Financial Management and Reporting (FMR)	399	Oversight of the Audit of the FY 2021 Defense Logistics Agency (DLA) General Fund Financial Statements	(b) (5) [redacted] The objective of the IPA's audit is to determine whether the FY 2021 Defense Logistics Agency, General Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the Defense Logistics Agency, General Fund financial statements for the fiscal years ending September 30, 2021 and September 30, 2020 and to determine whether the IPA complied with applicable auditing standards.	(b) (5) [redacted]			
2021	Audit	Financial Management and Reporting (FMR)	408	Oversight of the Audit of the FY 2021 Defense Logistics Agency (DLA) Working Capital Fund Financial Statements	(b) (5) [redacted]. The objective of the IPA's audit is to determine whether the FY 2021 Defense Logistics Agency, Working Capital Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the Defense Logistics Agency, Working Capital Fund financial statements for the fiscal years ending September 30, 2021 and September 30, 2020 and to determine whether the IPA complied with applicable auditing standards.				
2021	Audit	Financial Management and Reporting (FMR)	410	Oversight of the Audit of the FY 2021 Defense Information Systems Agency General Fund Financial Statements	(b) (5) [redacted]				
2021	Audit	Financial Management and Reporting (FMR)	411	Oversight of the Audit of the FY 2021 Department of the Army Working Capital Fund Financial Statements	(b) (5) [redacted]. The objective of the IPA's audit is to determine whether the FY 2021 AWCF financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the AWCF financial statements for the fiscal years ending September 30, 2021, and September 30, 2020, to determine whether the IPA complied with applicable auditing standards.				
2021	Audit	Financial Management and Reporting (FMR)	413	Oversight of the Audit of the FY 2021 Department of the Army General Fund Financial Statements	(b) (5) [redacted]. The objective of the IPA's audit is to determine whether the FY 2021 Army General Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the Army General Fund financial statements for the fiscal years ending September 30, 2021 and September 30, 2020, and to determine whether the IPA complied with applicable auditing standards.				
2021	Audit	Financial Management and Reporting (FMR)	415	Oversight of the Audit of the FY 2021 Military Retirement Fund Financial Statements	(b) (5) [redacted].				
2021	Audit	Financial Management and Reporting (FMR)	417	Oversight of the Audit of the FY 2021 Defense Logistics Agency (DLA) National Defense Stockpile Transaction Fund Financial Statements	(b) (5) [redacted] The objective of the IPA's audit is to determine whether the FY 2021 Defense Logistics Agency, Transaction Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the Defense Logistics Agency, Transaction Fund financial statements for the fiscal years ending September 30, 2021 and September 30, 2020 and to determine whether the IPA complied with applicable auditing standards.				
2021	Audit	Financial Management and Reporting (FMR)	418	Oversight of the FY 2021 Defense Logistics Agency Statement on Standards of Attestation Engagement No. 18, System and Organization Controls (SOC 1) Examination of the Wide Area Workflow (WAWF)	(b) (5) [redacted]. The objective of the IPA's attestation examination is to issue an opinion on the DLA's description of the WAWF and support services and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The objective of our oversight project is to provide contract oversight of the IPA's attestation examination and determine whether the IPA complied with applicable attestation standards.				

8. Improving DoD Financial Management and Budgeting

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2021	Audit	Financial Management and Reporting (FMR)	419	Oversight of the FY 2021 Defense Logistics Agency Statement on Standards of Attestation Engagement No. 18, System and Organization Controls (SOC 1) Examination of the Defense Agencies Initiative (DAI)	(b) (5) [redacted] The objective of the IPA's attestation examination is to issue an opinion on the DLA's description of the DAI and support services and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The objective of our oversight project is to provide contract oversight of the IPA's attestation examination and determine whether the IPA complied with applicable attestation standards.	(b) (5) [redacted]			
2021	Audit	Financial Management and Reporting (FMR)	421	Oversight of the Audit of the FY 2021 U.S. Army Corps of Engineers Civil Works Financial Statements	(b) (5) [redacted]				
2021	Audit	Financial Management and Reporting (FMR)	422	Oversight of the Audits of the FY 2021 U.S. Army Corps of Engineers Sub-Allotted Funds Financial Statements	(b) (5) [redacted]				
2021	Audit	Financial Management and Reporting (FMR)	423	Oversight of the FY 2021 Defense Logistics Agency Statement on Standards of Attestation Engagement No. 18, System and Organization Controls (SOC 1) Examination of the Defense Automatic Addressing System (DAAS)	(b) (5) [redacted]. The objective of the IPA's attestation examination is to issue an opinion on the DLA's description of the DAAS and support services and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The objective of our oversight project is to provide contract oversight of the IPA's attestation examination and determine whether the IPA complied with applicable attestation standards.				
2021	Audit	Financial Management and Reporting (FMR)	425	Audit of the DoD Agency-Wide Basic Financial Statements for the Fiscal Years Ending September 30, 2021, and September 30, 2020	The objective of this audit is to determine whether the DoD Agency-Wide Basic Financial Statements as of September 30, 2021 and 2020, taken as a whole, are presented fairly, in all material respects, and in conformity with accounting principles generally accepted in the United States of America. (b) (5) [redacted].				
2021	Audit	Financial Management and Reporting (FMR)	426	Attestation of the Agreed-Upon Procedures for Reviewing the FY 2021 Civilian Payroll Withholding	The objective of this agreed-upon procedures engagement is to assist the Office of Personnel Management in assessing whether retirement, health benefits, and life insurance withholdings and contributions as well as enrollment information submitted via the Semiannual Headcount Report by the Defense Finance and Accounting Service for FY 2021 were reasonable. (b) (5) [redacted].				
2021	Audit	Financial Management and Reporting (FMR)	427	Oversight of the Audit of the FY 2021 United States Special Operations Command (USSOCOM) General Fund Financial Statements	(b) (5) [redacted].				
2021	Audit	Financial Management and Reporting (FMR)	429	Oversight of the Audit of the FY 2021 Defense Information Systems Agency Working Capital Fund Financial Statements	(b) (5) [redacted].				

8. Improving DoD Financial Management and Budgeting

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2021	Audit	Financial Management and Reporting (FMR)	433	Oversight of the FY 2021 Defense Logistics Agency Statement on Standards of Attestation Engagement No. 18, System and Organization Controls (SOC 1) Examination of the Defense Property Accountability System (DPAS)	(b) (5) . The objective of the IPA's attestation examination is to issue an opinion on the DLA's description of the DPAS and support services and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The objective of our oversight project is to provide contract oversight of the IPA's attestation examination and determine whether the IPA complied with applicable attestation standards.	(b) (5)			
2021	Audit	Financial Management and Reporting (FMR)	436	Oversight of the Audit of the FY 2021 U.S. Transportation Command Working Capital Fund Financial Statements	(b) (5) .The objective of the IPA firm's audit is to determine whether the FY 2021 U.S. Transportation Command Working Capital Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. Our objective is to provide contract oversight of an IPA firm's audit of the U S. Transportation Command (USTRANSCOM) Working Capital Fund (WCF) Financial Statements for Fiscal Years ending September 30, 2021 and September 30, 2020 to determine if the IPA firm complied with applicable auditing standards.				
2021	Audit	Financial Management and Reporting (FMR)	438	Audit of the Defense Health Agency's Reporting of Improper Payment Estimates for the Military Health Benefits Program	The objective of this audit is to determine whether the Defense Health Agency (DHA) is accurately identifying and reporting improper payments as required by the Payment Integrity Information Act of 2019.				
2021	Audit	Financial Management and Reporting (FMR)	442	Oversight of the Audit of the FY 2021 Department of the Navy General Fund	(b) (5) The objective of the IPA's audit is to determine whether the FY 2021 Department of the Navy General Fund financial statements and related notes are presented fairly and in conformity with accounting principles generally accepted in the United States. The objective of our oversight project is to provide contract oversight of the IPA's audit of the Department of the Navy General Fund financial statements for the fiscal years ending September 30, 2021 and September 30, 2020 and to determine whether the IPA complied with applicable auditing standards.				
2021	Audit	Financial Management and Reporting (FMR)	559	(b) (5)	(b) (5) .				
2021	Audit	Readiness and Global Operations (RGO)	477	Interagency Coordination Group of Inspectors General for Guam Realignment Annual Report	The objective of this project is to compile a detailed statement of all FY 2021 obligations,expenditures, and revenues associated with military construction on Guam used tocreate the annual report of the Interagency Coordination Group of Inspectors Generalfor Guam Realignment by February 1, 2022.				
2021	Audit	Readiness and Global Operations (RGO)	658	Audit of the Combatant Command Execution of CARES Act Funding	The objective of this audit is to determine whether U.S. Southern Command, U S. Africa Command, and U.S. Indo-Pacific Command officials used Coronavirus Aid, Relief, and Economic Security Act funding to support the coronavirus disease 2019 pandemic response and operations in accordance with applicable Federal laws and DoD policies.				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	502	Evaluation of DoD Contracting Officer Actions on Contracts Terminated by the Government	The objective of this evaluation is to determine the extent to which DoD contracting officers complied with the Federal Acquisition Regulation (FAR), DoD policy, and Agency policy when they settled DoD contractor termination proposals. In addition, we will determine the extent to which DoD contracting officers complied with the FAR, DoD policy, and Agency policy when they settled DoD contractor termination proposals that may have been triggered by the COVID-19 pandemic.				

9. Restoring Trust and Confidence in the DoD

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Readiness and Global Operations (RGO)	656	Audit of the Military Entrance Processing Stations Efforts to Identify and Prevent Supremacist, Extremist, or Criminal Gang Members Prior to Selection into the Military Services	The objective of the audit is to determine whether the Military Entrance Processing Stations (MEPS) officials implemented policies and procedures that identify and prevent applicants with supremacist, extremist and or criminal gang member ideologies from being selected into the Military Services.	(b) (5)			
2022	Evaluations	Space, Intelligence, and Oversight (SIO)	493	Evaluation of the Management and Oversight of Undercover Operations by Military Criminal Investigative Organizations	The objectives of this evaluation are to determine whether the MCIOs have:1. Policies to ensure undercover operations are safely employed to obtain evidence and information in criminal investigations;2. Implemented recruitment, selection, training, and certification procedures for undercover agents and undercover teams; and3. Oversight procedures to ensure undercover operations are effective and comply with Military Service and MCIO policy.				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	365	Audit of Department of Defense Small Business Subcontracting	The objective of this audit is to determine whether DoD contracting officials awarded small business set-aside and sole-source contracts to contractors who complied with the established subcontracting limitations in accordance with applicable laws and regulations(b) (5)				
2021	Audit	Acquisition, Contracting, and Sustainment (ACS)	710	DoD Compliance with Whistleblower Protection Requirements	The objective of this audit it to determine whether DoD contracting officials are including required whistleblower clauses in contracts and ensuring that Defense contractors and subcontractors comply with the requirement to inform employees, in writing, of their whistleblower rights and remedies, as required by public law.				
2021	Audit	Cyberspace Operations (CSO)	361	Audit of U.S. Army Corps of Engineers Compliance with the Digital Accountability and Transparency Act of 2014	(b) (5)				
2021	Audit	Cyberspace Operations (CSO)	362	Audit of DoD Compliance with the Digital Accountability and Transparency Act of 2014	(b) (5)				
2021	Audit	Readiness and Global Operations (RGO)	604	Audit of Military Service Diversity and Inclusion Corrective Actions	The objective of this audit is to determine to what extent the Military Services implemented Diversity and Inclusion immediate actions approved by the Secretary of Defense (SECDEF) and agreed to by the Military Services in 2020.				
2021	Evaluations	Program, COCOM, and OCO Operations (PCOO)	533	Evaluation of the Department of Defense's (DoD) Implementation of the Military Leadership Diversity Commission's Recommendations and DoD's Diversity and Inclusion Strategic Plan	The objective of this evaluation is to determine the extent to which DoD implemented the objectives, strategic actions, and initiatives from the Military Leadership Diversity Commission's (MLDC) 2011 Final Report, œFrom Representation to Inclusion: Diversity Leadership for the 21st-Century Military,and the Department of Defense Diversity and Inclusion Strategic Plan (2012-2017).				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	561	External Peer Review of the Defense Commissary Agency Office of Internal Audit	The objective of this peer review is to determine whether the quality control program for the Defense Commissary Agency, Office of Internal Audit, for the period ending January 31, 2021, is designed to provide reasonable assurance that the policies and procedures related to the system of audit quality are suitably designed, operating effectively, and complied with in practice.				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	565	(b) (5)	(b) (5)				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	570	Quality Control Review of the Warren Averett, LLC Fiscal Year 2019 Single Audit of DEFENSEWERX, Inc.	The objective of this quality control review (QCR) is to determine whether Warren Averett, LLC performed the FY 2019 single audit of DEFENSEWERX, Inc (DWX) in accordance with auditing standards and Federal requirements.				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	571	External Peer Review of the National Guard Bureau Internal Review Office	The objective of this external peer review evaluation is to determine, for the 3-year period ended February 28, 2021 whether the quality control system for the National Guard Bureau Internal Review (NGB IR) Office was designed to provide reasonable assurance that the policies and procedures related to the system of quality control are suitably designed, operating effectively, and complied with in practice.				
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	585	Evaluation of the Department of Defense's Actions Regarding Unidentified Aerial Phenomena	See classified version of PPT				(b) (5)
2021	Evaluations	Space, Intelligence, and Oversight (SIO)	634	External Peer Review of the Defense Contract Management Agency Office of Internal Audit and Inspector General	The objective of this external peer review (peer review) is to determine whether the quality control program for the Defense Contract Management Agency Office of Internal Audit and Inspector General (DCMA OIA-IG), for the period ended May 31, 2021, is designed to provide reasonable assurance that the policies and procedures related to the system of audit quality are suitably designed, operating effectively, and complied with in practice.	(b) (5)			

9. Restoring Trust and Confidence in the DoD

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2020	Evaluations	Program, COCOM, and OCO Operations (PCOO)	539	Follow-up Evaluation of Report No. DODIG-2019-088, Evaluation of DoD Efforts to Combat Trafficking in Persons in Kuwait,â€ June 11, 2019	The objective of this followup evaluation is to determine whether DoD implemented corrective actions for the recommendations in the DODIG-2019-088, Evaluation of DoD Efforts to Combat Trafficking in Persons in Kuwait, June 11, 2019.	(b) (5)			

10. Developing an Adpative and Modern Workforce

Fiscal Year	Component	Directorate	Proposal Number	Title	Proposed Objective(s)	COVID-19 Related Proposal	Section 554 Related Proposal	Operation(s) Supported	Assessment Score
2022	Audit	Readiness and Global Operations (RGO)	641	Audit of DoD's Management of Science, Technology, Engineering, and Mathematics (STEM) Education Programs	The objective of this audit is to determine the extent to which the DoD developed measureable performance metrics, conducted evaluations, and reported on operations and results of DoD-funded STEM programs.	(b) (5)			
2020	Audit	Readiness and Global Operations (RGO)	534	Audit of the DoD's Strategic Workforce Planning for Overseas Civilian Positions	The objective of this audit is to determine whether the DoD conducts strategic workforce planning to hire and retain a competent overseas civilian workforce that effectively supports DoD's global mission and ongoing operations in accordance with DoD policies.				

Fiscal Year	Mission Area	Component	Proposal Number	Title
2022	Acquisition and Contracting	Audit	305	Audit of Department of Defense Commercial Item Part Pricing
2022	Acquisition and Contracting	Audit	367	Audit of Department of Defense Technical Data and License Rights to Sustain Systems
2022	Acquisition and Contracting	Audit	471	Audit of Performance Based Logistics Contracts for Systems, Subsystems, or Components
2022	Acquisition and Contracting	Audit	636	Audit of DoD Oversight of Energy Contracts
2022	Acquisition and Contracting	Audit	642	Audit of the Army's Integrated Visual Augmentation System (IVAS)
2022	Acquisition and Contracting	Audit	652	Followup Audit of the Navy's Oversight and Administration of Base Operating Support Services Contracts in Bahrain
2022	Acquisition and Contracting	Audit	659	Audit of Repair and Maintenance Requirements within Weapons Systems Acquisitions Contracts
2022	Acquisition and Contracting	Evaluations	697	Evaluation of DoD Contracting Officers' Use of Quick-Closeout Procedures in Class Deviation Authority 2019-0009 to Close DoD Contracts
2022	Acquisition and Contracting	Evaluations	699	Evaluation of Navy Contracting Officer Actions on Defense Contract Audit Agency Audit Findings and Recommendations
2021	Acquisition and Contracting	Audit	365	Audit of Department of Defense Small Business Subcontracting
2021	Acquisition and Contracting	Audit	370	Audit of Department of Defense Other Transactions and the Use of Non-traditional Contractors
2021	Acquisition and Contracting	Audit	455	Audit on the DoD Components' Award and Administration of Cost-Reimbursement Contracts
2021	Acquisition and Contracting	Audit	543	Audit of the Defense Ordnance Technology Consortium (DOTC) Award Process
2021	Acquisition and Contracting	Audit	560	Audit of the Office of Net Assessment's Contracting Administration Procedures
2021	Acquisition and Contracting	Audit	710	DoD Compliance with Whistleblower Protection Requirements
2021	Acquisition and Contracting	Evaluations	502	Evaluation of DoD Contracting Officer Actions on Contracts Terminated by the Government
2021	Acquisition and Contracting	Evaluations	513	Evaluation of the Department of Defense's Transition from a Trusted Foundry Model to a Zero-Trust Model for Procuring Microelectronics
2020	Acquisition and Contracting	Audit	152	Audit of the Air Force Remotely Piloted Aircraft Operations and Maintenance Contract
2020	Acquisition and Contracting	Audit	320	Audit of U.S. Army Corps of Engineers Border Infrastructure Contract
2020	Acquisition and Contracting	Audit	345	Audit of Contracts for Equipment and Supplies in Support of COVID-19
2020	Acquisition and Contracting	Audit	352	Audit of Sole-Source Depot Maintenance Contracts
2020	Acquisition and Contracting	Audit	412	Audit of DoD Implementation of Section 3610 Authorized by the Coronavirus Aid, Relief, and Economic Security Act
2020	Acquisition and Contracting	Audit	462	Audit of DoD Selection of Middle-Tier Acquisition Rapid Prototyping and Rapid Fielding Programs
2020	Acquisition and Contracting	Audit	531	Audit of Contracts Awarded and Administered by the Defense Media Activity
2020	Acquisition and Contracting	Audit	535	Audit of the Defense Logistics Agency Award and Management of Fuel Contracts in Areas of Contingency Operations
2020	Acquisition and Contracting	Evaluations	312	(U) Evaluation of the National Industrial Security Program Contract Classification System
2020	Acquisition and Contracting	Evaluations	348	Evaluation of Defense Logistics Agency (DLA) Oversight of Contracts for Ventilators and Respirators in Response to the COVID-19 Outbreak
2020	Acquisition and Contracting	Evaluations	523	Evaluation of Contract Administration and Oversight for Project Maven
2022	Aircraft	Audit	168	Audit of the Requirements Development for the MQ-25 Stingray
2022	Aircraft	Audit	470	Audit of Parts Purchased in Support of the F-35 Program
2022	Aircraft	Audit	654	Audit of B-52 Critical Spare Parts Inventory
2022	Aircraft	Evaluations	591	Evaluation of the Technology Readiness of the B-21 Raider Long Range Strike Bomber
2022	Aircraft	Evaluations	664	Evaluation of Service Capabilities to Counter Unmanned Aircraft Systems
2021	Aircraft	Audit	537	Audit of Navy and Marine Corps Actions to Address Corrosion on FA-18C-G Aircraft Project Proposal

Fiscal Year	Mission Area	Component	Proposal Number	Title
2022	Cyberspace	Audit	61	Audit of Cyber Security of Medical Devices at DoD Medical Treatment Facilities
2022	Cyberspace	Audit	125	Audit of U.S. Combatant Command Offensive Cyber Operations
2022	Cyberspace	Audit	181	Audit of DoD's Deconfliction of Cyberspace Operations
2022	Cyberspace	Audit	297	Audit of Security Controls Over the DoD Intelligence Community Enclaves
2022	Cyberspace	Audit	510	Audit of Combatant Command Training in a Contested Cyberspace Environment
2022	Cyberspace	Audit	511	Followup Audit on the DoD's Implementation of Cybersecurity Controls and Incident Response Procedures for Industrial Control Systems Supporting the Defense Critical Infrastructure
2022	Cyberspace	Audit	592	FY 2022 Audit of DoD's Compliance With the Federal Information Security Modernization Act of 2014
2022	Cyberspace	Audit	629	Summary of Reports and Testimonies Regarding DoD Cybersecurity from July 1, 2020, Through June 30, 2022
2022	Cyberspace	Audit	633	Audit of DoD Software Assurance Countermeasures During Weapon System Acquisitions
2022	Cyberspace	Audit	712	Audit of DoD's Actions to Implement Fifth-Generation (5G) Wireless Communications Technologies and Mitigate Associated Cybersecurity Risks
2021	Cyberspace	Audit	80	Audit of the Protection of Military Research Information and Technologies Developed by DoD Academic and Research Partners
2021	Cyberspace	Audit	406	Audit of DoD's Implementation of the Cybersecurity Information Sharing Act of 2015 (CISA)
2021	Cyberspace	Audit	459	Audit of the Implementation of Cybersecurity Controls for U.S Coast Guard Operated DoD Information Network (DoDIN) Systems
2021	Cyberspace	Audit	463	FY 2021 Audit of DoD's Compliance With the Federal Information Security Modernization Act of 2014 (FISMA)
2021	Cyberspace	Audit	478	Audit of the Defense Digital Service Support of DoD Programs and Operations
2021	Cyberspace	Audit	509	Audit of Management and Oversight of DoD Vulnerability and Mitigation Programs for Protecting the DoD Information Network
2021	Cyberspace	Audit	562	Audit of DoD Actions Taken to Protect the DoD Information Network Resulting From the SolarWinds Orion Compromise
2020	Cyberspace	Audit	66	Summary of Reports and Testimonies Regarding DoD Cybersecurity from July 1, 2019, Through June 30, 2020
2020	Cyberspace	Audit	68	Audit of DoD's Compliance with the Federal Information Security Modernization Act of 2014 (FISMA)
2020	Cyberspace	Audit	76	Audit on DoD Software Assurance Countermeasures During Weapon System Acquisitions
2020	Cyberspace	Audit	94	Audit of the National Background Investigation System Security and Interoperability
2020	Cyberspace	Audit	238	Audit of DoD's Acquisition and Use of Cloud Computing Services
2020	Cyberspace	Audit	296	Audit of the Collection, Analysis, Dissemination, and Security of Sensitive Information Maintained by the Defense Insider Threat Management and
2020	Cyberspace	Audit	316	Audit of Corrective Actions Taken by DoD Components in Response to Cybersecurity Vulnerabilities Identified During Cybersecurity Test and
2020	Cyberspace	Audit	346	Audit of Oversight of the Encore III Information Technology Service Task Orders
2020	Cyberspace	Audit	353	Audit of Contracts for DoD Information Technology Products and Services Procured by DoD Components in Response to the COVID-19 Pandemic
2020	Cyberspace	Audit	359	Audit of Maintaining Cybersecurity in the COVID-19 Telework Environment
2020	Cyberspace	Audit	364	Assessment of Access to DoD Information Technology and Communications During the COVID-19 Pandemic

Fiscal Year	Mission Area	Component	Proposal Number	Title
2022	Facilities and Infrastructure	Audit	72	Audit of the United States Army Corps of Engineers (USACE) Military Construction (MILCON) Projects
2022	Facilities and Infrastructure	Audit	393	Audit of Environmental Threats to Navy Shipyards
2022	Facilities and Infrastructure	Audit	643	Audit of European Deterrence Initiative (EDI) Military Construction Projects (MILCON)
2022	Facilities and Infrastructure	Audit	650	Audit of Infrastructure Resiliency at Military Installations in Southern California to Mitigate the Effects of Natural Disasters
2022	Facilities and Infrastructure	Audit	655	Summary Audit of Systemic Weaknesses in DoD's Oversight of Government Furnished Property
2022	Facilities and Infrastructure	Evaluations	483	Evaluation of the Department of Defense's Health, Safety, and Environmental Hazard Identification and Remediation Oversight Reform in Military Housing
2022	Facilities and Infrastructure	Evaluations	669	Evaluation of Security Controls at Sea Ports in the U.S. European Command Area of Responsibility
2021	Facilities and Infrastructure	Audit	452	Followup Audit of Army Oversight of Logistics Civil Augmentation Program V Government-Furnished Property in Afghanistan
2021	Facilities and Infrastructure	Audit	576	Audit of Medical Conditions of Residents in Privatized Military Housing
2021	Facilities and Infrastructure	Audit	579	Audit of Army Accountability of Government-Furnished Property Under Base Operations Contracts in Kuwait
2021	Facilities and Infrastructure	Audit	625	Audit of Cybersecurity of DoD Mobile Classified Devices
2021	Facilities and Infrastructure	Evaluations	563	Evaluation of Aircraft High-altitude Electromagnetic Pulse (HEMP) Life Cycle Testing and Test Facility Infrastructure
2021	Facilities and Infrastructure	Evaluations	567	Evaluation of the Department of Defense's Reform of Privatized Military Housing Oversight Related to Health, Safety, and Environmental Hazards
2021	Facilities and Infrastructure	Evaluations	572	Evaluation of the Air Force Selection Process for the Permanent Location of the U.S. Space Command Headquarters
2021	Facilities and Infrastructure	Evaluations	577	Evaluation of the Department of Defense's Efforts to Address the Climate Resilience of U.S. Military Installations in the Arctic and Sub-Arctic
2020	Facilities and Infrastructure	Audit	156	Audit of the DoD Infrastructure Planning in Australia
2020	Facilities and Infrastructure	Audit	347	Audit of U.S. Army Corps of Engineers Contract Quality Assurance Controls Over the Conversion of Alternate Care Sites for the COVID-19 Response
2020	Facilities and Infrastructure	Audit	381	Audit of the Disinfection of DoD Facilities in Response to the Coronavirus
2020	Facilities and Infrastructure	Evaluations	221	Evaluation of the Operational Support Capabilities of Naval Support Activity Bahrain Waterfront Facilities
2020	Facilities and Infrastructure	Evaluations	318	Evaluation of Per- and Polyflouroalkyl Substances (PFAS) Contamination at Military Installations
2020	Facilities and Infrastructure	Evaluations	324	Evaluation of the Ground Test and Evaluation Infrastructure Supporting Hypersonic Capabilities
2020	Facilities and Infrastructure	Evaluations	333	Evaluation of the DoD's Oversight of Privatized Military Housing Contracts
2020	Facilities and Infrastructure	Evaluations	382	Evaluation of DoD Medical Treatment Facility Challenges During the Coronavirus Disease 2019 (COVID-19)

Fiscal Year	Mission Area	Component	Proposal Number	Title
2022	Financial Management	Audit	584	Oversight of the Audit of the FY 2022 Department of the Air Force General Fund Financial Statements
2022	Financial Management	Audit	586	Oversight of the Audit of the FY 2022 Department of the Army General Fund Financial Statements
2022	Financial Management	Audit	587	Oversight of the Audit of the FY 2022 DoD Medicare-Eligible Retiree Health Care Fund Financial Statements
2022	Financial Management	Audit	588	Oversight of the Audit of the FY 2022 Defense Health Agency Contract Resource Management Financial Statements
2022	Financial Management	Audit	589	Oversight of the Audit of the FY 2022 Military Retirement Fund Financial Statements
2022	Financial Management	Audit	590	Attestation of the Agreed-Upon Procedures for Reviewing the FY 2022 Civilian Payroll Withholding
2022	Financial Management	Audit	594	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Defense Enterprise Accounting and Management System
2022	Financial Management	Audit	595	Oversight of the Audit of the FY 2022 Department of the Air Force Working Capital Fund Financial Statements
2022	Financial Management	Audit	596	Oversight of the Audit of the FY 2022 United States Marine Corps General Fund Financial Statements
2022	Financial Management	Audit	597	(b) (5) [redacted]
2022	Financial Management	Audit	598	Audit of the Department of Defense's Compliance in Fiscal Year 2022 With Payment Integrity Information Act Requirements
2022	Financial Management	Audit	599	Audit of the Reliability of the Improper Payment Estimates Reported for the Army Military Pay Program
2022	Financial Management	Audit	600	Oversight of the Audit of the FY 2022 Defense Health Program Financial Statements
2022	Financial Management	Audit	601	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the General Fund Enterprise Business System
2022	Financial Management	Audit	602	Oversight of the Audit of the FY 2022 Defense Information Systems Agency General Fund Financial Statements
2022	Financial Management	Audit	603	Oversight of the Audit of the FY 2022 Defense Information Systems Agency Working Capital Fund Financial Statements
2022	Financial Management	Audit	605	Oversight of the Audit of the FY 2022 U.S. Army Corps of Engineers-Civil Works Financial Statements
2022	Financial Management	Audit	606	Oversight of the Audits of the FY 2022 U.S. Army Corps of Engineers Sub-Allotted Funds Financial Statements
2022	Financial Management	Audit	607	Oversight of the Audit of the FY 2022 U.S. Transportation Command Working Capital Fund Financial Statements
2022	Financial Management	Audit	608	Oversight of the Audit of the FY 2022 Department of the Army Working Capital Fund
2022	Financial Management	Audit	609	Oversight of the FY 22 Department of Navy Working Capital Fund Financial Statement Audits and Examinations
2022	Financial Management	Audit	613	Oversight of the Audit of the FY 2022 Defense Logistics Agency General Fund Financial Statements.
2022	Financial Management	Audit	614	Oversight of the Audit of the FY 2022 Defense Logistics Agency Working Capital Fund Financial Statements.
2022	Financial Management	Audit	615	Oversight of the Audit of the FY 2022 Defense Logistics Agency National Defense Stockpile Transaction Fund Financial Statements.
2022	Financial Management	Audit	616	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Defense Agencies Initative
2022	Financial Management	Audit	618	Audit of the DoD Agency-Wide Basic Financial Statements for the Fiscal Years Ending September 30, 2022, and September 30, 2021

Fiscal Year	Mission Area	Component	Proposal Number	Title
2022	Financial Management	Audit	619	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Wide Area Workflow System
2022	Financial Management	Audit	620	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Defense Automatic Addressing System
2022	Financial Management	Audit	621	(b) (5) [redacted]
2022	Financial Management	Audit	622	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Defense Property Accountability System
2022	Financial Management	Audit	623	Oversight of the Audit of the FY 2022 United States Special Operations Command (USSOCOM) General Fund Financial Statements
2022	Financial Management	Audit	624	Oversight of the FY 22 Department of Navy General Fund Financial Statement Audits and Examinations
2022	Financial Management	Audit	630	Audit of DoD use of the Government Purchase Card in support of the Coronavirus Disease 2019 Pandemic Response
2022	Financial Management	Evaluations	504	Evaluation of Defense Contract Management Agency Preaward Financial Capability Reviews on Prospective DoD Contractors
2021	Financial Management	Audit	361	Audit of U.S. Army Corps of Engineers Compliance with the Digital Accountability and Transparency Act of 2014
2021	Financial Management	Audit	362	Audit of DoD Compliance with the Digital Accountability and Transparency Act of 2014
2021	Financial Management	Audit	371	Oversight of the Audit of the FY 2021 Department of the Air Force General Fund Financial Statements
2021	Financial Management	Audit	386	Oversight of the FY 2021 Department of the Air Force Statement on Standards of Attestation Engagement No. 18 Examination of the Defense Enterprise Accounting and Management System
2021	Financial Management	Audit	387	Oversight of the Audit of the FY 2021 Department of the Air Force Working Capital Fund Financial Statements
2021	Financial Management	Audit	389	Oversight of the Audit of the FY 2021 Defense Health Program General Fund Basic Financial Statements
2021	Financial Management	Audit	390	Attestation of Department of State Funds Transferred to DoD for Human Immunodeficiency Virus / Acquired Immune Deficiency Syndrome Prevention
2021	Financial Management	Audit	391	Oversight of the Audit of the FY 2021 DoD Medicare-Eligible Retiree Health Care Fund Basic Financial Statements
2021	Financial Management	Audit	392	Oversight of the Audit of the FY 2021 Defense Health Agency Contract Resource Management Basic Financial Statements
2021	Financial Management	Audit	397	Oversight of the Audit of the FY 2021 Department of the Navy Working Capital Fund Financial Statement Audit
2021	Financial Management	Audit	398	Oversight of the Audit of the FY 2021 United States Marine Corps General Fund Financial Statements
2021	Financial Management	Audit	399	Oversight of the Audit of the FY 2021 Defense Logistics Agency (DLA) General Fund Financial Statements
2021	Financial Management	Audit	408	Oversight of the Audit of the FY 2021 Defense Logistics Agency (DLA) Working Capital Fund Financial Statements
2021	Financial Management	Audit	410	Oversight of the Audit of the FY 2021 Defense Information Systems Agency General Fund Financial Statements
2021	Financial Management	Audit	411	Oversight of the Audit of the FY 2021 Department of the Army Working Capital Fund Financial Statements
2021	Financial Management	Audit	413	Oversight of the Audit of the FY 2021 Department of the Army General Fund Financial Statements
2021	Financial Management	Audit	415	Oversight of the Audit of the FY 2021 Military Retirement Fund Financial Statements
2021	Financial Management	Audit	417	Oversight of the Audit of the FY 2021 Defense Logistics Agency (DLA) National Defense Stockpile Transaction Fund Financial Statements

Fiscal Year	Mission Area	Component	Proposal Number	Title
2021	Financial Management	Audit	418	Oversight of the FY 2021 Defense Logistics Agency Statement on Standards of Attestation Engagement No. 18, System and Organization Controls (SOC 1) Examination of the Wide Area Workflow (WAWF)
2021	Financial Management	Audit	419	Oversight of the FY 2021 Defense Logistics Agency Statement on Standards of Attestation Engagement No. 18, System and Organization Controls (SOC 1) Examination of the Defense Agencies Initiative (DAI)
2021	Financial Management	Audit	421	Oversight of the Audit of the FY 2021 U.S. Army Corps of Engineers Civil Works Financial Statements
2021	Financial Management	Audit	422	Oversight of the Audits of the FY 2021 U.S. Army Corps of Engineers Sub-Allotted Funds Financial Statements
2021	Financial Management	Audit	423	Oversight of the FY 2021 Defense Logistics Agency Statement on Standards of Attestation Engagement No. 18, System and Organization Controls (SOC 1) Examination of the Defense Automatic Addressing System (DAAS)
2021	Financial Management	Audit	425	Audit of the DoD Agency-Wide Basic Financial Statements for the Fiscal Years Ending September 30, 2021, and September 30, 2020
2021	Financial Management	Audit	426	Attestation of the Agreed-Upon Procedures for Reviewing the FY 2021 Civilian Payroll Withholding
2021	Financial Management	Audit	427	Oversight of the Audit of the FY 2021 United States Special Operations Command (USSOCOM) General Fund Financial Statements
2021	Financial Management	Audit	429	Oversight of the Audit of the FY 2021 Defense Information Systems Agency Working Capital Fund Financial Statements
2021	Financial Management	Audit	432	Oversight of the FY 2021 Department of the Army Statement on Standards of Attestation Engagement No. 18, System and Organization Controls (SOC 1) Examination of the General Fund Enterprise Business System
2021	Financial Management	Audit	433	Oversight of the FY 2021 Defense Logistics Agency Statement on Standards of Attestation Engagement No. 18, System and Organization Controls (SOC 1) Examination of the Defense Property Accountability System (DPAS)
2021	Financial Management	Audit	436	Oversight of the Audit of the FY 2021 U.S. Transportation Command Working Capital Fund Financial Statements
2021	Financial Management	Audit	437	Oversight of the FY2021 Department of the Army Statement on Standards for Attestation Engagements No. 18, System and Organization Controls Examination of Controls of the System Supporting the Delivery of Munitions
2021	Financial Management	Audit	438	Audit of the Defense Health Agency's Reporting of Improper Payment Estimates for the Military Health Benefits Program
2021	Financial Management	Audit	442	Oversight of the Audit of the FY 2021 Department of the Navy General Fund
2021	Financial Management	Audit	544	(b) (5) [redacted]
2021	Financial Management	Audit	559	(b) (5) [redacted]
2021	Financial Management	Audit	610	Audit of the U.S. Northern Command Execution of the CARES Act Funding
2021	Financial Management	Audit	658	Audit of the Combatant Command Execution of CARES Act Funding
2020	Financial Management	Audit	63	Oversight of the Audit of the FY 2020 United States Air Force General Fund Financial Statements
2020	Financial Management	Audit	74	Contract Oversight of the Audit of the FY 2020 DoD Medicare-Eligible Retiree Health Care Fund Basic Financial Statements
2020	Financial Management	Audit	75	Contract Oversight of the Audit of the FY 2020 Defense Health Agency Contract Resource Management Basic Financial Statements
2020	Financial Management	Audit	77	Oversight of the Independent Public Accountant's (IPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Service Organization Controls (SOC) 1 Examination of Defense Agencies Initiative (DAI) for FY2020
2020	Financial Management	Audit	78	Oversight of the Independent Public Accountant's (IPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Service Organization Controls (SOC) 1 Examination of Wide Area Workflow (WAWF) for FY2020

Fiscal Year	Mission Area	Component	Proposal Number	Title
2020	Financial Management	Audit	79	Oversight of the Independent Public Accountant's (IPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Service Organization Controls (SOC) 1 Examination of Defense Automatic Addressing System (DAAS) for FY2020
2020	Financial Management	Audit	81	Oversight of the Audit of the FY 2020 United States Air Force Working Capital Fund Financial Statements
2020	Financial Management	Audit	82	Oversight of the FY 2020 Department of the Air Force Statement on Standards of Attestation Engagement No. 18 Examination of the Defense Enterprise Accounting and Management System.
2020	Financial Management	Audit	85	Oversight of the FY 2020 Department of the Army Statement on Standards for Attestation Engagements No. 18, System and Organization Controls Examination of the Systems Supporting the Delivery of Munitions Inventory Management Services
2020	Financial Management	Audit	86	Attestation Review of the DoD Counterdrug Program FY 2019 Performance Summary Report
2020	Financial Management	Audit	87	Attestation Review of the DoD Counterdrug Program FY 2019 Detailed Accounting Report
2020	Financial Management	Audit	88	Oversight of the Independent Public Accountant's (IPA) Financial Statement Audit of Defense Logistics Agency (DLA) General Fund for FY 2020
2020	Financial Management	Audit	89	Oversight of the FY 2020 United States Special Operations Command (USSOCOM) General Fund Statement
2020	Financial Management	Audit	90	Contract Oversight of the Audit of the FY 2020 Defense Health Program Enterprise General Fund Basic Financial Statements
2020	Financial Management	Audit	99	Oversight of the Audit of the FY 2020 U.S. Army Corps of Engineers Civil Works Basic Financial Statements
2020	Financial Management	Audit	101	Oversight of the Audits of the FY 2020 U.S. Army Corps of Engineers Sub-Allotted Funds Financial Statements
2020	Financial Management	Audit	105	Oversight of the FY 20 Department of the Navy Working Capital Fund Financial Statement Audits and Examinations
2020	Financial Management	Audit	106	Oversight of the Audit of the FY 2020 U.S. Transportation Command Working Capital Fund Financial Statements
2020	Financial Management	Audit	113	Oversight of the Independent Public Accountant's (IPA) Financial Statement Audit of Defense Logistics Agency (DLA) Working Capital Fund (WCF) for FY 2020
2020	Financial Management	Audit	115	Oversight of the Independent Public Accountant's (IPA) Financial Statement Audit of Defense Logistics Agency (DLA) Transaction Fund for FY 2020
2020	Financial Management	Audit	119	Oversight of the Independent Public Accountant's (IPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Service Organization Controls (SOC) 1 Examination of Service Owned Inventory in DLA Custody (SOIDC) for FY 2020
2020	Financial Management	Audit	121	Audit of the DoD Agency-Wide Basic Financial Statements for the Fiscal Years Ending September 30, 2020, and September 30, 2019
2020	Financial Management	Audit	131	Oversight of the Audit of the FY 2020 Department of the Army General Fund Financial Statements
2020	Financial Management	Audit	132	Oversight of the Independent Public Accountant (IPA) Engagement of Agreed-Upon Procedures (AUP) for Service Owned Inventory in DLA Custody (SOIDC) FY 2020
2020	Financial Management	Audit	136	Oversight of the Audit of the FY 2020 Defense Information Systems Agency (DISA) General Fund (GF) Financial Statements
2020	Financial Management	Audit	142	Oversight of the Audit of the FY 2020 Defense Information Systems Agency (DISA) Working Capital Fund (WCF) Financial Statements
2020	Financial Management	Audit	154	Audit of the Accuracy of the Improper Payment Estimates Reported for Mechanization of Contract Administration Services (MOCAS)
2020	Financial Management	Audit	162	Oversight of the FY 2020 Department of the Navy General Financial Statements Audits and Examinations

Fiscal Year	Mission Area	Component	Proposal Number	Title
2020	Financial Management	Audit	179	Oversight of the FY 2020 Department of the Army Statement on Standards of Attestation Engagement No. 18, System and Organization Controls Examination of the General Fund Enterprise Business System
2020	Financial Management	Audit	185	Oversight of the Audit of the FY 2020 Department of the Army Working Capital Fund Financial Statements
2020	Financial Management	Audit	213	Audit of the DoD FY 2020 Compliance with the Improper Payments Requirements
2020	Financial Management	Audit	240	Audit of the DoD Aviation Into-Plane Reimbursement (AIR) Card Program for Purchasing of Fuel and Non-Fuel Services
2020	Financial Management	Audit	264	Audit of the Accounting Corrections on the Standard Form 1081
2020	Financial Management	Audit	269	Oversight of the FY 2020 Military Retirement Fund FInancial Statements Audit
2020	Financial Management	Audit	270	Attestation of the Agreed-Upon Procedures for Reviewing the FY 2020 Civilian Payroll Withholding
2020	Financial Management	Audit	314	Audit of CECOM Billings to Customers for Industrial Services
2020	Financial Management	Audit	404	Audit of the Department of Defense Mission Assignments for Coronavirus Disease 2019 in the U.S. Northern Command Area of Responsibility
2020	Financial Management	Audit	409	Audit of Coalition Partner Reimbursements for Air Transportation Services in Afghanistan
2022	Health Care	Audit	209	Audit of the Oversight of Contractor Performance on the Military Health System - GENESIS Contract
2022	Health Care	Audit	628	Audit of DoD Medical Care for Victims of Sexual Assault
2022	Health Care	Evaluations	704	Evaluation of the Military Health System's Progress in the Transition of Operations to the Defense Health Agency
2022	Health Care	Evaluations	707	Evaluation of the DoD's use of Civilian and Veterans Affairs Partnerships to Meet Medical Provider Readiness Requirements
2021	Health Care	Audit	460	Audit of DoD's Exceptional Family Member Program in Overseas Locations
2021	Health Care	Audit	540	Audit of TRICARE Ambulance Transportation Reimbursements
2021	Health Care	Audit	545	Audit of the Reliability of the Department of Defense's Coronavirus Disease 2019 Patient Health Data
2021	Health Care	Audit	546	Audit of Substance Abuse (Alcohol) Program Screening and Treatment
2021	Health Care	Audit	569	Audit of DoD Implementation of the DoD Coronavirus Disease â€“ 2019 Vaccine Distribution Plan
2021	Health Care	Evaluations	694	Evaluation of Department of Defense Military Medical Treatment Facility Challenges During the Coronavirus Disease-2019 (COVID-19) Pandemic for Fiscal Year 2021
2021	Health Care	Evaluations	702	DoD and Service Identification and Screening of Service Members with Traumatic Brain Injuries (TBI)
2020	Health Care	Audit	67	Audit of TRICARE Telehealth Services
2020	Health Care	Audit	69	Audit of Access to DoD Health Care Records for High-Profile Individuals
2020	Health Care	Audit	344	Audit of Controls Over Costs for Health Care Claims for Services Related to COVID-19
2020	Health Care	Evaluations	308	Evaluation of Medical Resources and Guidance to Trainers at Recruit Training Centers in the DoD
2022	Intelligence	Evaluations	55	Evaluation of the Use of Compartmented Geospatial Intelligence Collection for Operation Inherent Resolve
2022	Intelligence	Evaluations	486	Evaluation of Intelligence Support, Communication, and Information Sharing Across the Hypersonic Community on Adversary Hypersonic Weapon Systems
2022	Intelligence	Evaluations	665	Evaluation of National Geospatial-Intelligence Agency Support to Military Operations
2022	Intelligence	Evaluations	688	(~~CUI~~) Evaluation of Identity Intelligence and Threats to Intelligence Operatives and Operations
2022	Intelligence	Evaluations	691	Evaluation of the Office of Special Investigations Counterintelligence Response to Espionage and Criminal Threats Posed by the People's Republic of China
2022	Intelligence	Evaluations	692	Evaluation of the Exploitation of Foreign Source Materiels Obtained by the DoD

Fiscal Year	Mission Area	Component	Proposal Number	Title
2021	Intelligence	Evaluations	585	Evaluation of the Department of Defense's Actions Regarding Unidentified Aerial Phenomena
2020	Intelligence	Evaluations	44	Evaluation of the Combatant Commands' Intelligence Interrogations
2020	Intelligence	Evaluations	245	Evaluation of the Foreign Influence in DoD Research and Development
2020	Intelligence	Evaluations	284	(U/~~FOUO~~) (b)(5) [redacted]
2020	Intelligence	Evaluations	310	(U) Evaluation of ISR Sensor Supply Chain Lifetime Purchases (Classified Title on SIPR)
2020	Intelligence	Evaluations	331	Evaluation of the National Security Agency Integration of Artificial Intelligence
2020	Intelligence	Evaluations	532	Evaluation of the Office of Net Assessment
2020	Land Vehicles	Audit	322	Followup Audit on the Implemented Recommendations Addressing the Army and Marine Corps Joint Light Tactical Vehicle (JLTV)
2022	Law Enforcement	Evaluations	660	Evaluation of the Military Criminal Investigative Organization's Confidential Source Programs
2022	Law Enforcement	Evaluations	689	Evaluation of the Air Force Office of Special Investigations (OSI) Internal Control Systems for Criminal Investigations and Supporting Programs
2022	Law Enforcement	Evaluations	693	Evaluation of the DoD Military Working Dog (MWD) Program
2021	Law Enforcement	Evaluations	224	Evaluation of DoD Law Enforcement Organizations' Response to Active Shooter Incidents
2021	Law Enforcement	Evaluations	230	Evaluation of the Military Criminal Investigative Organization (MCIO) Major Procurement Fraud Programs
2020	Law Enforcement	Evaluations	319	Evaluation of the U.S. Military Support of Security Operations at the U.S. Southern Border
2022	Operations and Readiness	Audit	60	Audit of the Accuracy of Classifying and Reporting of Service Members' Individual Medical Readiness.
2022	Operations and Readiness	Audit	329	Audit of Individual Preparedness to Conduct Extreme Cold Weather Operations
2022	Operations and Readiness	Audit	640	Audit of the National Defense Space Architecture Interoperability with DoD Programs of Record
2022	Operations and Readiness	Audit	644	Audit of U.S. European Command's Missile Defense Capabilities
2022	Operations and Readiness	Audit	645	Audit of Army Oversight of DoD Language Interpretation and Translation Enterprise II Contract
2022	Operations and Readiness	Audit	647	Audit of Test, Measurement, and Diagnostic Equipment Used to Maintain Weapon Systems
2022	Operations and Readiness	Audit	649	Audit of Energy Resilience in Emergency Preparedness Plans
2022	Operations and Readiness	Evaluations	317	Evaluation of U.S. Central Command's Defense of Critical Assets Within its Area of Responsibility Against Missiles and Unmanned Aircraft Systems
2022	Operations and Readiness	Evaluations	375	Evaluation of U.S. Special Operations Command Joint Military Information Support Operations Web Operations Center (JMWC)
2022	Operations and Readiness	Evaluations	667	Evaluation of the Effectiveness of Security Force Assistance Brigades
2022	Operations and Readiness	Evaluations	695	Evaluation of the Military Sealift Command's Surge Sealift Readiness in a Global Crisis
2021	Operations and Readiness	Audit	368	Audit of the Department of Defense's Implementation of Predictive Maintenance Strategies to Support Weapon System Sustainment
2021	Operations and Readiness	Audit	454	Audit of Training Ranges Supporting Units in the U.S. European Command
2021	Operations and Readiness	Audit	477	Interagency Coordination Group of Inspectors General for Guam Realignment Annual Report
2021	Operations and Readiness	Audit	530	Audit of DoD Education Activity Return-to-School Plans
2021	Operations and Readiness	Audit	558	Audit of the Accuracy and Reliability of the Defense Enrollment Eligibility Reporting System Data
2021	Operations and Readiness	Audit	604	Audit of Military Service Diversity and Inclusion Corrective Actions

Fiscal Year	Mission Area	Component	Proposal Number	Title
2021	Operations and Readiness	Evaluations	662	Follow-Up on Trans-Africa Airlift Support in the U.S. Africa Command (DoDIG-2018-116)
2020	Operations and Readiness	Audit	96	Audit of the Military Service's Planning Processes for C5ISR Reparable Items at the Depot Level
2020	Operations and Readiness	Audit	148	Audit of Entitlements and Allowances for Deployed Reserve Service Members
2020	Operations and Readiness	Audit	160	Follow Up Audit of the U.S. Army's Management of the Heavy Lift VIII Contract to Meet Changing Middle East Mission
2020	Operations and Readiness	Audit	304	Interagency Coordination Group of Inspectors General for GuamRealignment Annual Report
2020	Operations and Readiness	Audit	338	(b) (5) [redacted]
2020	Operations and Readiness	Audit	356	(b) (5) [redacted]
2020	Operations and Readiness	Audit	360	Audit of the Impact of Coronavirus Disease 2019 on Basic Military Training
2020	Operations and Readiness	Audit	380	Audit of Infectious Disease Medical Treatment Capabilities at Al Udeid Air Base
2020	Operations and Readiness	Audit	402	Audit of U.S. Transportation Command Cargo Scheduling Effectiveness
2020	Operations and Readiness	Audit	445	Audit of the Department of Defense Management of Depot-Level Reparables (DLRs) for Major-End Items
2020	Operations and Readiness	Audit	475	Audit of the DoD Military Installations Preparedness for Public Health Emergency Readiness
2020	Operations and Readiness	Evaluations	39	(U) Evaluation of Kinetic Targeting Processes in the USAFRICOM Area of Responsibility
2020	Operations and Readiness	Evaluations	315	Evaluation of the U.S. Navy's P-8 Aircraft Readiness to Meet the U.S. European Command's Anti-Submarine Warfare Requirements
2020	Operations and Readiness	Evaluations	358	Evaluation of U.S. Combatant Command Responses to the COVID-19 Pandemic
2020	Operations and Readiness	Evaluations	366	Evaluation of the Navy's Plans and Response to the Coronavirus-Disease-2019 Outbreak Onboard Ships
2022	Personnel	Audit	641	Audit of DoD's Management of Science, Technology, Engineering, and Mathematics (STEM) Education Programs
2022	Personnel	Audit	656	Audit of the Military Entrance Processing Stations Efforts to Identify and Prevent Supremacist, Extremist, or Criminal Gang Members Prior to Selection into the Military Services
2022	Personnel	Evaluations	493	Evaluation of the Management and Oversight of Undercover Operations by Military Criminal Investigative Organizations
2022	Personnel	Evaluations	632	Evaluation of the Military Criminal Investigative Organizations' Adult Sexual Assault Investigations
2021	Personnel	Audit	564	(b) (5) [redacted]
2021	Personnel	Evaluations	485	Evaluation of the Department of Defense Voting Assistance Program for Calendar Year 2020
2021	Personnel	Evaluations	494	Evaluation of the DoD's Implementation of Suicide Prevention Resources for Transitioning Uniformed Service Members
2021	Personnel	Evaluations	533	Evaluation of the Department of Defense's (DoD) Implementation of the Military Leadership Diversity Commission's Recommendations and DoD's Diversity and Inclusion Strategic Plan
2021	Personnel	Evaluations	557	Systems Review of the U.S. Army Criminal Investigation Division's Internal Control Systems for Criminal Investigations and Supporting Programs
2020	Personnel	Audit	140	Audit of the Award and Administration of National Guard Youth Challenge Program Cooperative Agreements
2020	Personnel	Audit	309	Audit of the DoD's Recruitment and Retention of the Civilian Cyber Workforce
2020	Personnel	Audit	355	Audit of Dual-Status Commanders for use in Defense Support of Civil Authorities

Fiscal Year	Mission Area	Component	Proposal Number	Title
2020	Personnel	Audit	534	Audit of the DoD's Strategic Workforce Planning for Overseas Civilian Positions
2020	Personnel	Audit	536	(b) (5) [redacted]
2020	Personnel	Evaluations	220	Evaluation of the Special Victim Investigation and Prosecution (SVIP) Capability within the Department of Defense
2020	Personnel	Evaluations	233	Evaluation of the DoD's Handling of Incidents of Sexual Assault Against (or Involving) Midshipmen at the United States Naval Academy
2020	Personnel	Evaluations	294	Evaluation of DoD Voting Assistance Programs for Calendar Year 2019
2020	Personnel	Evaluations	339	(b) (5) [redacted]
2020	Personnel	Evaluations	357	Evaluation of Traumatic Brain Injury Screening in the U.S. Central Command Area of Responsibility
2020	Personnel	Evaluations	539	Follow-up Evaluation of Report No. DODIG-2019-088, Evaluation of DoD Efforts to Combat Trafficking in Persons in Kuwait, June 11, 2019
2022	Policy	Audit	653	Audit of the Department of Defense's Internal Controls of Financial Assistance Awards
2022	Policy	Evaluations	663	External Inspection and Evaluation Peer Review of the Department of Interior Office of the Inspector General
2022	Policy	Evaluations	670	Quality Control Review on Single Audit of Advanced Technology International
2022	Policy	Evaluations	676	Quality Control Review on Single Audit of the Geneva Foundation
2022	Policy	Evaluations	677	Quality Control Review on Single Audit of the United Service Organization, Inc.
2022	Policy	Evaluations	683	External Peer Review of the U.S Special Operations Command Office of Inspector General, Audit Division
2022	Policy	Evaluations	684	Oversight of the Naval Audit Service External Peer Review
2022	Policy	Evaluations	685	External Peer Review of the Army Internal Review Program
2022	Policy	Evaluations	686	External Peer Review of the Defense Logistics Agency Office of Inspector General Audit Organization
2021	Policy	Audit	612	Audit of the DoD Approval Process for Companies Designated as Critical to Maintaining National Security to Obtain Coronavirus Aid, Relief, and Economic Security Act Section 4003 Loans
2021	Policy	Evaluations	490	External Peer Review on the Missile Defense Agency Internal Review Office
2021	Policy	Evaluations	547	Evaluation of DoD Efforts to Develop and Implement Policy and Procedures Addressing Ideological Extremism within the U.S. Armed Forces
2021	Policy	Evaluations	548	Evaluation of U.S. Central Command and U.S. Special Operations Command Implementation of DoD's Law of War Program
2021	Policy	Evaluations	550	Review of DoD's Implementation of Executive Order 13950, Combating Race and Sex Stereotyping, September 22, 2020
2021	Policy	Evaluations	561	External Peer Review of the Defense Commissary Agency Office of Internal Audit
2021	Policy	Evaluations	565	(b) (5) [redacted]
2021	Policy	Evaluations	570	Quality Control Review of the Warren Averett, LLC Fiscal Year 2019 Single Audit of DEFENSEWERX, Inc.
2021	Policy	Evaluations	571	External Peer Review of the National Guard Bureau Internal Review Office

Fiscal Year	Mission Area	Component	Proposal Number	Title
2021	Policy	Evaluations	634	External Peer Review of the Defense Contract Management Agency Office of Internal Audit and Inspector General
2020	Policy	Evaluations	46	External Peer Review of the Defense Logistics Agency Audit Function
2020	Policy	Evaluations	47	External Peer Review of the Defense Information Systems Agency Office of the Inspector General Audit Organization
2020	Policy	Evaluations	48	External Peer Review of the Defense Finance and Accounting Service Internal Review Audit Organization
2020	Policy	Evaluations	52	(b) (5) [redacted]
2020	Policy	Evaluations	53	(b) (5) [redacted]
2020	Policy	Evaluations	54	Follow-up on Summary Report on Audit Quality
2020	Policy	Evaluations	225	Quality Control Review on Single Audit of the American Society for Engineering Education
2020	Policy	Evaluations	227	(b) (5) [redacted]
2020	Policy	Evaluations	247	External Peer Review of the Department of State OIG Office of Inspections
2020	Policy	Evaluations	496	(b) (5) [redacted]
2020	Policy	Evaluations	522	Air Force Audit Agency Peer Review Oversight
2020	Policy	Mission Support Team (MST)	328	(b) (5) [redacted]
2020	Policy	Mission Support Team (MST)	529	(b) (5) [redacted]
2022	Security Cooperation	Audit	293	Audit of DoD Cybersecurity Requirements for the Foreign Military Sales Program
2022	Security Cooperation	Audit	474	Audit of U.S. Indo-Pacific Command's Efforts to Implement the Pacific Deterrence Initiative
2021	Security Cooperation	Audit	467	Audit of Vetting of International Military Students Enrolled in United States-Based Training Programs and Accompanying Family Members
2021	Security Cooperation	Audit	551	Audit of the DoD Counter-Islamic State of Iraq and Syria Train and Equip Fund Stipends to the Vetted Syrian Opposition
2021	Security Cooperation	Overseas Contingency Operations	626	Evaluation of Combatant Command Communication Challenges with Foreign Nation Partners During the COVID-19 Pandemic
2020	Security Cooperation	Audit	528	Audit of DoD's Management of Global Train and Equip Program Resources Provided to U.S. Africa Command (USAFRICOM)
2022	Space	Evaluations	480	Evaluation of the Space Fence Space Situational Awareness System
2021	Space	Audit	476	Audit of DoD Maintenance of Space Launch Equipment and Facilities
2021	Space	Evaluations	479	Evaluation of the DoD's Strategy to Test Space-Based Systems in Contested Space Environments
2022	Supply Chain	Audit	637	Followup Audit of the Defense Logistics Agency Aviation Product Quality Deficiency Report Processing
2022	Supply Chain	Audit	639	Audit of the Defense Logistics Agency Storage of Program Executive Office Ground Combat Systems Equipment
2022	Supply Chain	Audit	646	Audit of Defense Logistics Agency Storage and Disposal of Hazardous Material
2022	Supply Chain	Audit	648	(b) (5) [redacted]
2022	Supply Chain	Audit	711	Audit of the Defense Logistics Agency's Cybersecurity Supply Chain Risk Management
2022	Supply Chain	Evaluations	303	Evaluation of a Classified NGA Program
2022	Supply Chain	Evaluations	666	Evaluation of the Readiness of U.S. Marine Corps' Pre-Positioned War Reserve Stocks in Support of USINDOPACOM's Operation Plans
2022	Supply Chain	Evaluations	696	Evaluation of the Department of Defense's Laser Interferometry Upgrades and Compliance with DoD Policy Requirements for Mitigating Supply Chain Risks and Foreign Influence
2022	Supply Chain	Evaluations	709	Evaluation of Governance and Protection of Department of Defense Research and Development of Emergent Technology

Fiscal Year	Mission Area	Component	Proposal Number	Title
2021	Supply Chain	Audit	405	Audit of the Tracking, Recovery, and Reuse of Department of Defense-Owned Shipping Containers
2021	Supply Chain	Audit	439	Audit of the Reuse of Excess Department of Defense Property
2021	Supply Chain	Audit	449	Audit of the DoD Federal Mall Purchases
2021	Supply Chain	Evaluations	498	Evaluation of the DoD's Mitigation of Foreign Suppliers in the Pharmaceutical Supply Chain
2021	Supply Chain	Evaluations	552	Evaluation of U.S. Special Operations Command's Supply Chain Risk Management for the Security, Acquisition, and Delivery of Specialized Equipment
2021	Supply Chain	Evaluations	575	Evaluation of the DoD's Actions to Develop Interoperable Joint Logistics Enterprise Systems and Tools for Demand Forecasting
2020	Supply Chain	Audit	109	(b) (5) [redacted]
2020	Supply Chain	Audit	538	Audit of the Department of Defense Coronavirus Aid, Relief, and Economic Security Act Awards to Increase the Defense Industrial Base Manufacturing Capacity
2020	Supply Chain	Evaluations	376	(b) (5) [redacted]
2022	Weapons and Munitions	Audit	472	Audit of the Acquisition of the Air Force Three Dimensional Expeditionary Long-Range Radar
2022	Weapons and Munitions	Audit	593	Oversight of the Statement on Standards for Attestation Engagements No. 18 Examination of the Army's System Supporting the Delivery of Munitions Inventory Management Services
2022	Weapons and Munitions	Evaluations	488	(U) Evaluation of the North Warning System
2022	Weapons and Munitions	Evaluations	687	Evaluation of the DoD's Efforts to Modernize the U.S. Nuclear Command, Control, and Communication System
2022	Weapons and Munitions	Evaluations	698	Evaluation of the Nuclear Certification of the Long Range Standoff Missile (LRSO)
2022	Weapons and Munitions	Evaluations	701	Evaluation of Sustaining Engineering Actions for the Minuteman III Missile Program
2022	Weapons and Munitions	Evaluations	703	Evaluation of Sustaining Engineering Actions for the Air Force's Upgraded Early Warning Radar System
2021	Weapons and Munitions	Evaluations	611	Evaluation of the Notification Procedures that the DoD Has in Place for the Presidential Emergency Satchel
2020	Weapons and Munitions	Evaluations	33	Evaluation of the Aircraft Monitor and Control System's Nuclear Certification
2020	Weapons and Munitions	Evaluations	35	Evaluation of the Navy Airborne Support to the Survivable Nuclear Command and Control System

From	'(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>, "Stebbins, Steven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "Roark, Michael J., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Stone, Randolph R., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "FitzHarris, Leo J., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>
Cc	'(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>
Subject	'They want people to take them seriously': Space Force wary of taking over UFO mission
Date	Mon, 9 Aug 2021 19:02:00 +0000
Message-Id	<eb6c5c8e5e034d9cb5fbaacc5d8dc11f@DODIG.MIL>

FYSA.

'They want people to take them seriously': Space Force wary of taking over UFO mission

BY BRYAN BENDER | 08/09/2021 02:02 PM EDT

The Pentagon is considering giving the Space Force a greater role in a stepped-up effort to track and investigate reports of UFOs. But the newest military branch isn't over the moon about the idea.

Space Force leaders are still struggling to rebrand an organization that has been lampooned since before its birth. Now, they are conflicted about becoming the military's go-to on what the Pentagon now calls "unmanned aerial phenomena," according to five current and former officials taking part in the discussions.

Advocates for the Space Force taking over for the Navy, which is currently leading the Pentagon's task force respons ble for studying them, believe the new service is better suited to oversee a more robust effort aimed at collecting information on UFOs, and that its association with a topic of such public fascination, particularly among young people, could even boost recruiting.

"It makes perfect sense," said one former intelligence official who is advising the military in the planning, citing its more expansive geographic responsibilities than other military branches and access to global - and even galactic - surveillance technologies through the U.S. Space Command. "There is no limit to the Space Force mission. It doesn't have a geographic boundary l ke the other services."

But the former official also said some fear it will only deepen the branch's public relations challenge by providing more material for the jokes, science-fiction-themed memes and other forms of popular ridicule that the Space Force has endured since it was championed by then-President Donald Trump in 2018, who made it an applause line in his political rallies.

"They really are sensitive to that," the former official said. "They want people to take them seriously. They don't want to do anything that is embarrassing. But this is national security. This is their job."

The deliberations over what to do next about the unexplained sightings of high performance aircraft are part of a new push to establish a more permanent government research effort.

A June report to Congress from the director of national intelligence concluded that all but one of 144 UFO sightings that were reviewed could not be explained, including 18 that appeared to exhibit advanced properties. The unclassified summary stated that "we currently lack sufficient information in our dataset to attribute incidents to specific explanations." It also concluded that the unknown craft "clearly pose a safety of flight issue and may pose a challenge to U.S. national security."

In response, the undersecretary of defense for intelligence and security is developing a plan to "formalize the mission" after being instructed by Deputy Defense Secretary Kathleen Hicks.

In a memo to senior military leaders following the report's release, Hicks sought a plan "for the establishment and operation of the new activity, to include the organizational alignment, resources and staffing required, as we ll as any necessary authorities."

The issue has primarily been overseen by a temporary Pentagon UAP Task Force that was stood up in 2020 and led by the Navy, whose pilots, radars and other surveillance systems have compiled most of the recent reports of unexplained sightings.
The Pentagon has provided few details about the deliberations over what will replace the task force. "Planning for an activity to take over the UAPTF's mission is ongoing," said Pentagon spokesperson Susan Gough.
The Space Force declined to address the internal deliberations. The Department of the Air Force, which oversees the Space Force, also deferred questions to Gough.
Congress, which requested the UAP report, is also planning to play more of a role.
The Senate's version of the fiscal 2022 Intelligence Act includes several provisions on the subject, including requiring classified reports to Congress on UAP sightings and analysis every quarter, as well as calling on all agencies to share any data they have so that a more comprehensive UFO file can be compiled for further study.
A congressional staffer also told POLITICO the classified portion of the bill includes a provision outlining more parameters for tackling the subject over the longer term, including recommending additional funding to finance t he effort.
A former Pentagon official also said he expects there will also be legislative guidance on UAPs in a final version of the National Defense Authorization Act.
But in addition to the Space Force, which works in tandem with the newly reestablished U.S. Space Command, officials are considering a number of military and intelligence organizations at this early stage that could take the lead or combine their efforts in a new organization.
One is the secretive Space Security and Defense Program, which reports to both the Pentagon and the director of national intelligence, which oversees all spy agencies.
The outfit has a broad writ to assess potential space threats and also has authority to award contracts to develop new collection capabilities. Other candidates for a greater role in overseeing UFO issues are the Defense Intelligence Agency, which studies foreign weapons systems and has a history of researching such sightings, as well as the North American Aerospace Defense Command in Colorado, which is respons ble for defending the nation's airspace.
Chris Mellon, a former senior Pentagon intelligence official and congressional staffer who has been advising the military on the topic, said whoever is tasked with leading a more permanent effort needs to be willing to work cl osely with numerous military, intelligence and law enforcement agencies across the government as well as the academic and scientific communities and the public.
"NORAD would seem to make sense, but again its willingness to share information with other organizations is questionable. Still, they have money and contracting authority and the heft needed to make changes to the status quo if they were willing to aggressively pursue the issue," he wrote in a recent blog post.
"Regardless," he added, "the first and most important step for Congress to take is to either identify a permanent home for the mission or require DoD and the CI [intelligence community] to do so and to explain their resulting rationale with the oversight committees."
V,
(b) (6)
, Communications
Office of Legislative Affairs and Communications
(b) (6) , DoD Office of Inspector General
O: (b) (6)
(b) (6) @dodig.mil
Connect with us @dod_ig and LinkedIn at DoD Inspector General
http://www.dodig.mil/Mailing-Lists/

From	'(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>, "Stebbins, S teven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OI G DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" < (b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "Garrison, Marguerite C., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, "Roa rk, Michael J., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Stone, Randolph R., SES, OIG DoD" <(b) (6) @DODIG.MIL>, "Hadjiyane, Paul, SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>
Cc	"Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., O IG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
Subject	Congress weighs whistleblower safeguards after Trump saga
Date	Thu, 12 Aug 2021 19:14:32 +0000
Message-Id	<c6f6c3c76443487d8d46beb823d2533c@DODIG.MIL>

Good afternoon.
FYSA, below is a CQ article on provisions related to whistleblower protections included in the SSCI bill for the FY 2022 Intelligence Authorization Act. The relevant sections in the attached bill are sections 321 to 324. OLAC will continue to monitor this bill and provide updates.
###
Congress weighs whistleblower safeguards after Trump saga
Aug. 12, 2021 ? 2:51 p.m. By John M. Donnelly, CQ
The Senate Intelligence Committee wants to give whistleblowers who work for U.S. intelligence agencies groundbreaking new protections, a response to what members see as flaws in the process revealed in the leadup to President Donald Trump's first impeachment.
The committee's new intelligence authorization bill would enable spy-agency whistleblowers to more easily communicate concerns straight to Congress. It would make disclosure of the identity of an anonymous whistleblower a crime. It would empower anyone whose name was revealed against his or her will to fight back in court.
And it would make clear that no administration official can kill a complaint by simply keeping it from reaching Capitol Hill.
The proposed changes are in the fiscal 2022 intelligence measure (S 2610), which the panel approved late last month.
The legislation was fueled by concerns that arose in 2019, when a report from an anonymous whistleblower from one of the intelligence agencies became the center of Washington political debate and eventually led to Trump's first impeachment trial in January 2020.
On Aug. 12, 2019, exactly two years ago, that whistleblower contended Trump had sought to use U.S. aid and other levers of American power to coerce Ukraine's leaders into manufacturing dirt on Joe Biden, then his leading Democratic rival in his reelection bid.
Kept from Congress
For more than a month, Joseph Maguire, the acting director of national intelligence, withheld the complaint from Congress with the help of the Justice Department. It was only delivered to Congress on Sept. 25, 2019, after lawmakers filed a subpoena and press disclosures had revealed the outlines of the complaint.
Meanwhile, Trump and his allies in Congress sought to discover and disclose the whistleblower's identity, particularly after a right-wing outlet reported a name and work history without direct confirmation. And Trump even hinted the person should be executed.

Sen. Rand Paul, R-Ky., threatened to publicly disclose the name. GOP Reps. Devin Nunes of California and Jim Jordan of Ohio appeared to be trying to force a witness at one House Intelligence Committee hearing to divulge the whistleblower's identity. Those efforts drew objections from Democrats and many Republicans at the time.
This week, California Democrat Adam B. Schiff, the chairman of the House Intelligence Committee who was the lead manager of Trump's first impeachment, told CQ Roll Call in a statement that his panel will review the new Senate proposal, and he expects to propose his own legislation addressing this issue and others that affect congressional oversight.
"The abuses of the Trump administration laid bare the urgent need to bolster whistleblower protections, including within the Intelligence Community," Schiff said. "IC personnel who courageously expose wrongdoing and illegality through the whistleblower process must never fear retribution for doing the right thing."
Mark Zaid, an attorney who represented the Ukraine whistleblower, called the Senate's new intelligence bill a positive step.
"The objective they are trying to achieve is spot-on necessary, because of what we encountered during the impeachment case," Zaid said in an interview. "They are filling in the holes we had to jump around."
Proposed new system
Longtime whistleblower advocate Ron Wyden, D-Ore., the Senate Intelligence Committee member who wrote the panel's proposed changes to laws governing disclosure of wrongdoing in intelligence agencies, said they would "address abuses by the Trump Administration."
Currently, whistleblowers in the spy agencies can send only "urgent" concerns to Congress?and only after routing them through senior officials.
Specifically, an inspector general, either from a particular spy agency or of the overall intelligence community, has to review the complaint to determine that it is urgent enough for the Intelligence panels to consider. If it is deemed urgent, then the agency head must send the complaint to the Intelligence committees.
But the process did not work as planned in 2019. Maguire withheld the Ukraine complaint from Congress, while Justice Department attorneys argued that the matter was not urgent, among other claims.
Experts pointed out at the time that only inspectors general can determine urgency, and that Maguire did not have authority to do anything other than convey the report to Capitol Hill.
The new Senate bill would retain the existing process for complaints concerning urgent issues, but would make plain that the intelligence agencies' inspectors general "shall have sole authority" to determine a complaint's urgency.
Crucially, the legislation would add a new, alternative avenue for whistleblowers to inform Congress of alleged wrongdoing, whether the issue could be deemed urgent or not.
In particular, the intelligence authorization measure would allow whistleblowers in the spy agencies to communicate concerns to the Intelligence committees via newly created "security officers" at their agencies.
But if those security officers do not provide the whistleblowers with "procedural direction" on how to notify Congress within 30 days ? or that direction is "insufficient" ? then the employee can go straight to the House and Senate Intelligence committees with the concerns.
Moreover, the bill would seek to protect intelligence community whistleblowers ? both agency employees and contractors ? from the "knowing and willful" disclosure of their identities against their wishes, which could be retaliation against someone who discloses.
Up until now, experts said, a prohibition against disclosure of a whistleblower's name has not been previously made plain in law.
The bill also would give whistleblowers whose identities are revealed against their will access to courts to seek redress ? the first time intelligence community whistleblowers would have such an explicit right, the experts said.
Clearer and stronger
Kel McClanahan, executive director of National Security Counselors, a law firm that represents defense and intelligence personnel, said the measure clarifies and strengthens existing law.
"This bill will go a great distance toward harmonizing the treatment an Agriculture Department employee and a CIA employee get for the same protected activity," he said.
The bill also contains a provision that would seek to improve the process by which intelligence agency employees can contest revocation or suspension of their security clearances, which is frequently how agency bosses punish whistleblowers for disclosing problems, McClanahan said.
Nevertheless, spy-agency whistleblowers still must contest their actions inside their agencies, often appealing to the very people who are accused of wrongdoing, several legal experts said.
Unlike federal workers in other agencies, intelligence personnel cannot appeal to the Office of Special Counsel or the Merit Systems Protection Board, said Melissa Wasser, policy counsel for the Project on Government Oversight, which advocates for stronger protections for personnel who disclose wrongdoing.

“Our top recommendation when it comes to intelligence community whistleblowers is making sure that they're able to get some level of independent enforcement in the process,” Wasser said.
Way forward
The outlook for the Senate Intelligence Committee’s provisions is not yet clear. The House Intelligence Committee has not yet marked up its intelligence authorization bill.
Similar measures to add protections for spy agency whistleblowers have been proposed but defeated previously on Capitol Hill, due partly to GOP objections, including from Nunes, the top Republican on the House Intelligence Committee. Nunes did not reply to a request for comment.
Marco Rubio of Florida, the top Republican on the Senate panel, supports the new proposals.
The measure “improves the Intelligence Community’s (IC’s) Inspectors General authorities and enhances the congressional intelligence committees’ already-vigilant oversight of IC whistleblower actions,” a Rubio aide said in a statement to CQ Roll Call.
The House Committee on Oversight and Reform approved in June a bill (HR 2988) by New York Democrat Carolyn B. Maloney, the panel’s chairwoman, that addresses whistleblowing laws for non-intelligence employees. The Senate has yet to mirror that effort.
But intelligence agency whistleblowers are different. Their disclosures often involve classified data. If such whistleblowers do not have a way to tell Congress secret information without ruining their lives, then they often t urn to the press or to outfits such as Wikileaks, potentially jeopardizing U.S. security.
Yet, as the 2019 Ukraine whistleblower case showed, previous laws and presidential directives have still not created a system that assures whistleblowers not only that they will be protected but also that their concerns will be addressed, analysts said.
“Everyone who cares about congressional oversight understands that whistleblowers shouldn’t fear either retaliation or futility for stepping forward,” said Irvin McCullough, an expert on laws governing whistleblowers with the Government Accountability Project, a group that provides them legal representation and advocacy.
“We are all better off?and our country more secure?when we protect those who make congressional oversight possible.”
Respectfully,

(b) (6)
[redacted]
Office of Legislative Affairs & Communications
Department of Defense Office of Inspector General
4800 Mark Center Drive
Alexandria, VA 22350
(b) (6)
(b) (6) [redacted] @dodig.mil

.....

Attachment Name : S. 2610 - IAA for FY22.pdf

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 116

117TH CONGRESS
1ST SESSION

S. 2610

To authorize appropriations for fiscal year 2022 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

IN THE SENATE OF THE UNITED STATES

AUGUST 4, 2021

Mr. WARNER, from the Select Committee on Intelligence, reported the following original bill; which was read twice and placed on the calendar

---

A BILL

To authorize appropriations for fiscal year 2022 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Intelligence Authorization Act for Fiscal Year 2022".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—INTELLIGENCE ACTIVITIES

Sec. 101. Authorization of appropriations.
Sec. 102. Classified Schedule of Authorizations.
Sec. 103. Intelligence Community Management Account.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Sec. 201. Authorization of appropriations.

TITLE III—GENERAL INTELLIGENCE MATTERS

Subtitle A—Intelligence Community Matters

Sec. 301. Increasing agricultural and commercial intelligence measures.
Sec. 302. Plan for allowing contracts with providers of services relating to sensitive compartmented information facilities.
Sec. 303. Plan to establish commercial geospatial intelligence data and services program office.
Sec. 304. Investment strategy for commercial geospatial intelligence services acquisition.
Sec. 305. Central Intelligence Agency Acquisition Innovation Center report, strategy, and plan.
Sec. 306. Improving authorities relating to national counterintelligence and security.
Sec. 307. Removal of Chief Information Officer of the Intelligence Community from level IV of the Executive Schedule.
Sec. 308. Requirements relating to construction of facilities to be used primarily by intelligence community.
Sec. 309. Director of National Intelligence support for intelligence community diversity, equity, inclusion, and accessibility activities.
Sec. 310. Establishment of Diversity, Equity, and Inclusion Officer of the Intelligence Community.
Sec. 311. Clarification of authority of National Reconnaissance Office.
Sec. 312. Director of National Intelligence declassification review of information relating to terrorist attacks of September 11, 2001.
Sec. 313. Establishment of Chaplain Corps of the Central Intelligence Agency.
Sec. 314. Pilot program on recruitment and retention in Office of Intelligence and Analysis of the Department of the Treasury.
Sec. 315. Pilot program on student loan repayment at Office of Intelligence and Analysis of Department of the Treasury.
Sec. 316. Prohibition on collection and analysis of United States persons' information by intelligence community based on First Amendment-protected activities.
Sec. 317. Sense of the Senate on the use of intelligence community resources for collection, assessment, and analysis of information pertaining exclusively to United States persons absent a foreign nexus.

Subtitle B—Inspector General of the Intelligence Community

Sec. 321. Submittal of complaints and information by whistleblowers in the intelligence community to Congress.
Sec. 322. Definitions and authorities regarding whistleblower complaints and information of urgent concern received by Inspectors General of the intelligence community.
Sec. 323. Harmonization of whistleblower protections.
Sec. 324. Prohibition against disclosure of whistleblower identity as reprisal against whistleblower disclosure by employees and contractors in intelligence community.

Subtitle C—Reports and Assessments Pertaining to the Intelligence Community

Sec. 331. Report on efforts to build an integrated hybrid space architecture.
Sec. 332. Report on Project Maven transition.
Sec. 333. Assessment of intelligence community counternarcotics capabilities.
Sec. 334. Assessment of intelligence community's intelligence-sharing relationships with Latin American partners in counternarcotics.
Sec. 335. Report on United States Southern Command intelligence capabilities.
Sec. 336. Director of National Intelligence report on trends in technologies of strategic importance to United States.
Sec. 337. Report on Nord Stream II companies and intelligence ties.
Sec. 338. Assessment of Organization of Defensive Innovation and Research activities.
Sec. 339. Report on intelligence community support to Visas Mantis program.
Sec. 340. Plan for artificial intelligence digital ecosystem.
Sec. 341. Study on utility of expanded personnel management authority.
Sec. 342. Assessment of role of foreign groups in domestic violent extremism.
Sec. 343. Report on the assessment of all-source cyber intelligence information, with an emphasis on supply chain risks.
Sec. 344. Review of National Security Agency and United States Cyber Command.
Sec. 345. Support for and oversight of Unidentified Aerial Phenomena Task Force.
Sec. 346. Publication of unclassified appendices from reports on intelligence community participation in Vulnerabilities Equities Process.
Sec. 347. Report on future structure and responsibilities of Foreign Malign Influence Center.

Subtitle D—People's Republic of China

Sec. 351. Assessment of posture and capabilities of intelligence community with respect to actions of the People's Republic of China targeting Taiwan.
Sec. 352. Plan to cooperate with intelligence agencies of key democratic countries regarding technological competition with People's Republic of China.
Sec. 353. Assessment of People's Republic of China genomic collection.
Sec. 354. Updates to annual reports on influence operations and campaigns in the United States by the Chinese Communist Party.
Sec. 355. Report on influence of People's Republic of China through Belt and Road Initiative projects with other countries.
Sec. 356. Study on the creation of an official digital currency by the People's Republic of China.

Sec. 357. Report on efforts of Chinese Communist Party to erode freedom and autonomy in Hong Kong.
Sec. 358. Report on targeting of renewable sectors by China.

TITLE IV—ANOMALOUS HEALTH INCIDENTS

Sec. 401. Definition of anomalous health incident.
Sec. 402. Assessment and report on interagency communication relating to efforts to address anomalous health incidents.
Sec. 403. Advisory panel on the Office of Medical Services of the Central Intelligence Agency.
Sec. 404. Joint task force to investigate anomalous health incidents.
Sec. 405. Reporting on occurrence of anomalous health incidents.
Sec. 406. Access to certain facilities of United States Government for assessment of anomalous health conditions.

TITLE V—SECURITY CLEARANCES AND TRUSTED WORKFORCE

Sec. 501. Exclusivity, consistency, and transparency in security clearance procedures, and right to appeal.
Sec. 502. Federal policy on sharing of derogatory information pertaining to contractor employees in the trusted workforce.
Sec. 503. Performance measures regarding timeliness for personnel mobility.
Sec. 504. Governance of Trusted Workforce 2.0 initiative.

TITLE VI—OTHER INTELLIGENCE MATTERS

Sec. 601. National Technology Strategy.
Sec. 602. Improvements relating to continuity of Privacy and Civil Liberties Oversight Board membership.
Sec. 603. Air America.
Sec. 604. Access by Comptroller General of the United States to certain cybersecurity records.
Sec. 605. Reports on intelligence support for and capacity of the Sergeants at Arms of the Senate and the House of Representatives and the United States Capitol Police.
Sec. 606. Study on vulnerability of Global Positioning System to hostile actions.
Sec. 607. Authority for transportation of federally owned canines associated with force protection duties of intelligence community.

SEC. 2. DEFINITIONS.

In this Act:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term ''congressional intelligence committees'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(2) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given such term in such section.

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 2022 for the conduct of the intelligence and intelligence-related activities of the following elements of the United States Government:

(1) The Office of the Director of National Intelligence.

(2) The Central Intelligence Agency.

(3) The Department of Defense.

(4) The Defense Intelligence Agency.

(5) The National Security Agency.

(6) The Department of the Army, the Department of the Navy, and the Department of the Air Force.

(7) The Coast Guard.

(8) The Department of State.

(9) The Department of the Treasury.

(10) The Department of Energy.

(11) The Department of Justice.

(12) The Federal Bureau of Investigation.

(13) The Drug Enforcement Administration.

(14) The National Reconnaissance Office.

(15) The National Geospatial-Intelligence Agency.

(16) The Department of Homeland Security.

(17) The Space Force.

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

(a) SPECIFICATIONS OF AMOUNTS.—The amounts authorized to be appropriated under section 101 for the conduct of the intelligence activities of the elements listed in paragraphs (1) through (17) of section 101, are those specified in the classified Schedule of Authorizations prepared to accompany this Act.

(b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AUTHORIZATIONS.—

(1) AVAILABILITY.—The classified Schedule of Authorizations referred to in subsection (a) shall be made available to the Committee on Appropriations of the Senate, the Committee on Appropriations of the House of Representatives, and to the President.

(2) DISTRIBUTION BY THE PRESIDENT.—Subject to paragraph (3), the President shall provide for suitable distribution of the classified Schedule of Authorizations referred to in subsection (a), or of ap-

propriate portions of such Schedule, within the executive branch of the Federal Government.

(3) LIMITS ON DISCLOSURE.—The President shall not publicly disclose the classified Schedule of Authorizations or any portion of such Schedule except—

(A) as provided in section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 3306(a));

(B) to the extent necessary to implement the budget; or

(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2022 the sum of $615,600,000.

(b) CLASSIFIED AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2022 such additional amounts as are

specified in the classified Schedule of Authorizations referred to in section 102(a).

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund $514,000,000 for fiscal year 2022.

TITLE III—GENERAL INTELLIGENCE MATTERS

Subtitle A—Intelligence Community Matters

SEC. 301. INCREASING AGRICULTURAL AND COMMERCIAL INTELLIGENCE MEASURES.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Agriculture, Nutrition, and Forestry, the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Committee on Banking, Housing, and Urban Affairs, and the Select Committee on Intelligence of the Senate; and

(2) the Committee on Agriculture, the Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Financial Services, and the Permanent Select Committee on Intelligence of the House of Representatives.

(b) REPORT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with other appropriate Federal Government entities, shall submit to the appropriate committees of Congress a report detailing the options for the intelligence community to improve intelligence support to the Department of Agriculture and the Department of Commerce.

(c) FORM.—The report required under subsection (b) shall be submitted in unclassified form, but may include a classified annex, if necessary.

SEC. 302. PLAN FOR ALLOWING CONTRACTS WITH PROVIDERS OF SERVICES RELATING TO SENSITIVE COMPARTMENTED INFORMATION FACILITIES.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services of the Senate; and

(3) the Committee on Armed Services of the House of Representatives.

(b) PLAN REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a plan for allowing elements of the intelligence community to contract with providers of services relating to sensitive compartmented information facilities for use of those facilities by businesses and organizations on contracts at multiple security levels.

(c) ELEMENTS.—The plan required by subsection (b) shall include the following:

(1) An explanation of how the Director of National Intelligence will leverage the contracting methodology the National Reconnaissance Office has used to provide leased sensitive compartmented information facility space to businesses and organizations.

(2) Policy and budget guidance to incentivize Federal agencies to implement the plan required by subsection (b).

SEC. 303. PLAN TO ESTABLISH COMMERCIAL GEOSPATIAL INTELLIGENCE DATA AND SERVICES PROGRAM OFFICE.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

(b) PLAN REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of the National Reconnaissance Office and the Director of the National Geospatial-Intelligence Agency, in consultation with the Director of National Intelligence, shall jointly develop and submit to the appropriate committees of Congress a plan to establish an office described in subsection (c).

(c) OFFICE DESCRIBED.—An office described in this subsection is a co-located joint commercial geospatial intelligence data and services program office at the National Geospatial-Intelligence Agency, the head of which shall be a representative from the National Geospatial-Intelligence

Agency and the deputy head of which shall be a representative from the National Reconnaissance Office.

(d) CONTENTS.—The plan required by subsection (b) shall include the following:

(1) Milestones for implementation of the plan.

(2) An updated acquisition strategy that—

(A) provides for an annual evaluation of new capabilities with opportunities to contract with or terminate use of commercial providers at least annually; and

(B) considers efficiencies to be gained from closely coordinated acquisitions of geospatial intelligence data and services.

(3) A plan for the establishment of a commercial geospatial intelligence data innovation fund equaling at least 10 percent of the total commercial data investment of the National Reconnaissance Office to enable the rapid procurement of data supporting emerging global mission requirements.

SEC. 304. INVESTMENT STRATEGY FOR COMMERCIAL GEOSPATIAL INTELLIGENCE SERVICES ACQUISITION.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

(b) STRATEGY REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of the National Geospatial-Intelligence Agency, in consultation with the Director of National Intelligence and the Secretary of Defense, shall submit to the appropriate committees of Congress an investment strategy for the acquisition of commercial geospatial intelligence data services and analytics by the National Geospatial-Intelligence Agency.

(c) CONTENTS.—The strategy required by subsection (b) shall include the following:

(1) A plan to increase purchases of unclassified geospatial intelligence data services and analytics to meet global mission requirements of the National Geospatial-Intelligence Agency while maximizing enterprise access agreements for procured data and services.

(2) An articulation of the relationship between geospatial intelligence data and services and how

such data and services are purchased, identifying in particular any challenges to procuring such services independent of the underlying data.

SEC. 305. CENTRAL INTELLIGENCE AGENCY ACQUISITION INNOVATION CENTER REPORT, STRATEGY, AND PLAN.

(a) REQUIREMENT FOR REPORT AND STRATEGY.—Not later than 120 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall submit to the congressional intelligence committees—

(1) a report stating the mission and purpose of the Acquisition Innovation Center of the Agency; and

(2) a strategy for incorporating the Acquisition Innovation Center into the standard operating procedures and procurement and acquisition practices of the Agency.

(b) REQUIREMENT FOR IMPLEMENTATION PLAN.—Not later than 120 days after the date of the enactment of this Act, the Director shall, using the findings of the Director with respect to the report submitted under subsection (a)(1), submit to the congressional intelligence committees an implementation plan that addresses—

(1) how the Director will ensure the contracting officers of the Agency and the technical representatives of the Acquisition Innovation Center for the contracting officers have access to the technical expertise required to inform requirements development, technology maturity assessments, and monitoring of acquisitions;

(2) how the plan specifically applies to technical industries, including telecommunications, software, aerospace, and large-scale construction; and

(3) projections for resources necessary to support the Acquisition Innovation Center, including staff, training, and contracting support tools.

SEC. 306. IMPROVING AUTHORITIES RELATING TO NATIONAL COUNTERINTELLIGENCE AND SECURITY.

(a) DUTIES OF THE DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER.—Section 902(c) of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3382(c)) is amended by adding at the end the following:

''(5) To organize and lead strategic planning for counterintelligence activities in support of National Counterintelligence Strategy objectives and other national counterintelligence priorities by inte-

grating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities, within and among Federal agencies.''.

(b) CHANGES TO THE FUNCTIONS OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER.—

(1) EVALUATION OF IMPLEMENTATION OF NATIONAL COUNTERINTELLIGENCE STRATEGY.—Paragraph (3) of section 904(d) of such Act (50 U.S.C. 3383(d)) is amended to read as follows:

''(3) IMPLEMENTATION OF NATIONAL COUNTERINTELLIGENCE STRATEGY.—To evaluate on an ongoing basis the implementation of the National Counterintelligence Strategy by the intelligence community and other appropriate elements of the United States Government and to submit to the President, the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), the National Security Council, the Director of the Office of Management and Budget, and the National Counterintelligence Policy Board periodic reports on such evaluation, including a discussion of any shortfalls in the implementation of the Strategy and recommendations for remedies for such shortfalls.''.

(2) NATIONAL COUNTERINTELLIGENCE PROGRAM BUDGET.—Paragraph (5) of such section is amended—

(A) in subparagraph (A)—

(i) by inserting ''oversee and'' before ''coordinate''; and

(ii) by inserting ''in furtherance of the National Counterintelligence Strategy and other strategic counterintelligence priorities'' before ''of the Department of Defense''; and

(B) in subparagraph (C), by striking ''the National Security Council'' and inserting ''the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), the National Security Council, the Director of the Office of Management and Budget, and the National Counterintelligence Policy Board''.

(3) NATIONAL COUNTERINTELLIGENCE OUTREACH, WATCH, AND WARNING.—

(A) COUNTERINTELLIGENCE VULNERABILITY RISK ASSESSMENTS.—Subparagraph (A) of paragraph (7) of such section is amended by striking ''surveys of the vulnerability of the

United States Government, and the private sector,'' and inserting ''counterintelligence risk assessments and surveys of the vulnerability of the United States''.

(B) OUTREACH.—Subparagraph (B) of such paragraph is amended to read as follows:

''(B) OUTREACH.—

''(i) OUTREACH PROGRAMS AND ACTIVITIES.—To carry out and coordinate, consistent with other applicable provisions of law and in consultation with appropriate Federal departments and agencies, outreach programs and outreach activities on counterintelligence to other elements of the United States Government, State, local, and Tribal governments, foreign governments and allies of the United States, the private sector, and United States academic institutions.

''(ii) PUBLIC WARNINGS.—To coordinate the dissemination to the public of warnings on intelligence threats to the United States.''.

SEC. 307. REMOVAL OF CHIEF INFORMATION OFFICER OF THE INTELLIGENCE COMMUNITY FROM LEVEL IV OF THE EXECUTIVE SCHEDULE.

Section 5315 of title 5, United States Code, is amended by striking ''Chief Information Officer of the Intelligence Community''.

SEC. 308. REQUIREMENTS RELATING TO CONSTRUCTION OF FACILITIES TO BE USED PRIMARILY BY INTELLIGENCE COMMUNITY.

Section 602(a) of the Intelligence Authorization Act for Fiscal Year 1995 (50 U.S.C. 3304(a)) is amended—

(1) in paragraph (1), by striking ''$5,000,000'' and inserting ''$6,000,000''; and

(2) in paragraph (2), by striking ''$5,000,000'' and inserting ''$6,000,000''.

SEC. 309. DIRECTOR OF NATIONAL INTELLIGENCE SUPPORT FOR INTELLIGENCE COMMUNITY DIVERSITY, EQUITY, INCLUSION, AND ACCESSIBILITY ACTIVITIES.

(a) IN GENERAL.—Title XI of the National Security Act of 1947 (50 U.S.C. 3231 et. seq.) is amended by adding at the end the following:

"SEC. 1111. SUPPORT FOR INTELLIGENCE COMMUNITY DIVERSITY, EQUITY, INCLUSION, AND ACCESSIBILITY ACTIVITIES.

"(a) DEFINITION OF COVERED WORKFORCE ACTIVITIES.—In this section, the term 'covered workforce activities' includes—

"(1) activities relating to the recruitment or retention of personnel in the workforce of the intelligence community; and

"(2) activities relating to the workforce of the intelligence community and diversity, equity, inclusion, or accessibility.

"(b) AUTHORITY TO SUPPORT COVERED WORKFORCE ACTIVITIES.—Notwithstanding any other provision of law and subject to the availability of appropriations made available to the Director of National Intelligence for covered workforce activities, the Director may, with or without reimbursement, support such covered workforce activities of the various elements of the intelligence community as the Director determines will benefit the intelligence community as a whole.".

(b) CLERICAL AMENDMENT.—The table of contents at the beginning of such Act is amended by inserting after the item relating to section 1110 the following:

"Sec. 1111. Support for intelligence community diversity, equity, inclusion, and accessibility activities.".

SEC. 310. ESTABLISHMENT OF DIVERSITY, EQUITY, AND INCLUSION OFFICER OF THE INTELLIGENCE COMMUNITY.

(a) IN GENERAL.—Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.) is amended by inserting after section 103J (50 U.S.C. 3034a) the following:

"SEC. 103K. DIVERSITY, EQUITY, AND INCLUSION OFFICER OF THE INTELLIGENCE COMMUNITY.

"(a) DIVERSITY, EQUITY, AND INCLUSION OFFICER OF THE INTELLIGENCE COMMUNITY.—Within the Office of the Director of National Intelligence, there is a Diversity, Equity, and Inclusion Officer of the Intelligence Community who shall be appointed by the Director of National Intelligence.

"(b) DUTIES.—The Diversity, Equity, and Inclusion Officer of the Intelligence Community shall—

"(1) serve as the principal advisor to the Director of National Intelligence and the Principal Deputy Director of National Intelligence on diversity, equity, and inclusion in the intelligence community;

"(2) lead the development and implementation of strategies and initiatives to advance diversity, equity, and inclusion in the intelligence community; and

''(3) perform such other duties, consistent with paragraphs (1) and (2), as may be prescribed by the Director.

''(c) ANNUAL REPORTS TO CONGRESS.—Not less frequently than once each year, the Diversity, Equity, and Inclusion Officer of the Intelligence Community shall submit to the congressional intelligence communities a report on the implementation of the strategies and initiatives developed pursuant to subsection (b)(2) and the execution of related expenditures.

''(d) PROHIBITION ON SIMULTANEOUS SERVICE AS OTHER DIVERSITY, EQUITY, AND INCLUSION OR EQUAL EMPLOYMENT OPPORTUNITY OFFICER.—An individual serving in the position of Diversity, Equity, and Inclusion Officer of the Intelligence Community may not, while so serving, serve as either the Diversity, Equity, and Inclusion Officer or the Equal Employment Opportunity Officer of any other department or agency, or component thereof, of the United States Government.''.

(b) CLERICAL AMENDMENT.—The table of contents at the beginning of such Act is amended by inserting after the item relating to section 103J the following:

''Sec. 103K. Diversity, Equity, and Inclusion Officer of the Intelligence Community.''.

(c) LIMITATION.—None of the funds authorized to be appropriated by this Act may be used to increase the num-

ber of full-time equivalent employees of the Office of the Director of National Intelligence in order to carry out section 103K of such Act, as added by subsection (a).

SEC. 311. CLARIFICATION OF AUTHORITY OF NATIONAL RECONNAISSANCE OFFICE.

Section 106A of the National Security Act of 1947 (50 U.S.C. 3041a) is amended—

(1) by redesignating subsection (d) as subsection (e); and

(2) by inserting after subsection (c) the following new subsection (d):

''(d) CLARIFICATION OF AUTHORITY.—

''(1) PROHIBITION ON TRANSFER OF ELEMENTS.—No element of the National Reconnaissance Office may be transferred to the Space Force.

''(2) NO EFFECT ON AUTHORITIES.—Nothing in chapter 908 of title 10, United States Code, shall affect the authorities, duties, or responsibilities of the Director of the National Reconnaissance Office, including with respect to the authority of the Director to operate a unified organization to carry out the research, development, test, evaluation, acquisition, launch, deployment, and operations of overhead reconnaissance systems and related data processing facilities of the National Reconnaissance Office.''.

SEC. 312. DIRECTOR OF NATIONAL INTELLIGENCE DECLASSIFICATION REVIEW OF INFORMATION RELATING TO TERRORIST ATTACKS OF SEPTEMBER 11, 2001.

(a) DECLASSIFICATION REVIEW REQUIRED.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall, in coordination with the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, and the heads of such other elements of the intelligence community as the Director of National Intelligence considers appropriate, commence a declassification review, which the Director of National Intelligence shall complete not later than 120 days after the date of the enactment of this Act, to determine what additional information relating to the terrorist attacks of September 11, 2001, can be appropriately declassified and shared with the public.

(b) INFORMATION COVERED.—The information reviewed under subsection (a) shall include the following:

(1) Information relating to the direction, facilitation, and other support provided to the individuals who carried out the terrorist attacks of September 11, 2001.

(2) Information from Operation Encore and the PENTTBOM investigation of the Federal Bureau of Investigation.

(c) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on the findings of the Director with respect to the declassification review conducted under subsection (a).

SEC. 313. ESTABLISHMENT OF CHAPLAIN CORPS OF THE CENTRAL INTELLIGENCE AGENCY.

The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.) is amended by adding at the end the following:

"SEC. 26. CHAPLAIN CORPS AND CHIEF OF CHAPLAINS.

''(a) ESTABLISHMENT OF CHAPLAIN CORPS.—There is in the Agency a Chaplain Corps for the provision of spiritual or religious pastoral services.

''(b) CHIEF OF CHAPLAINS.—The head of the Chaplain Corps shall be the Chief of Chaplains, who shall be appointed by the Director.

''(c) STAFF AND ADMINISTRATION.—

''(1) STAFF.—The Director may appoint and fix the compensation of such staff of the Chaplain Corps as the Director considers appropriate, except that the Director may not—

''(A) appoint more than 10 full-time equivalent positions; or

''(B) provide basic pay to any member of the staff of the Chaplain Corps at an annual rate of basic pay in excess of the maximum rate of basic pay for grade GS–15 as provided in section 5332 of title 5, United States Code.

''(2) ADMINISTRATION.—The Director may—

''(A) reimburse members of the staff of the Chaplain Corps for work-related travel expenses;

''(B) provide security clearances to such members; and

''(C) furnish such physical workspace at the headquarters building of the Agency as the Director considers appropriate.''.

SEC. 314. PILOT PROGRAM ON RECRUITMENT AND RETENTION IN OFFICE OF INTELLIGENCE AND ANALYSIS OF THE DEPARTMENT OF THE TREASURY.

(a) PILOT PROGRAM REQUIRED.—The Assistant Secretary for Intelligence and Analysis in the Department of the Treasury shall carry out a pilot program to assess the feasibility and advisability of using adjustments of rates of pay to recruit and retain staff for high-demand posi-

tions in the Office of Intelligence and Analysis of the Department of the Treasury.

(b) DURATION.—The Assistant Secretary shall carry out the pilot program required by subsection (a) during the 4-year period beginning on the date of the enactment of this Act.

(c) ADDITIONAL PAY.—Under the pilot program required by subsection (a), the Assistant Secretary shall, notwithstanding any provision of title 5, United States Code, governing the rates of pay or classification of employees in the executive branch, prescribe the rate of basic pay for financial and cyber intelligence analyst positions designated under subsection (d) at rates—

(1) not greater than 130 percent of the maximum basic rate of pay and locality pay that such positions would otherwise be eligible for; and

(2) not greater than the rate of basic pay payable for level II of the Executive Schedule under section 5313 of title 5, United States Code.

(d) DESIGNATED POSITIONS.—

(1) IN GENERAL.—Except as provided in paragraph (2), under the pilot program required by subsection (a), the Assistant Secretary shall designate not fewer than 5 percent and not more than 25 percent of the total number of positions in the Office,

including positions to be filled by new hires, as financial or cyber intelligence analyst positions eligible for the additional pay under subsection (c).

(2) CURRENT EMPLOYEES.—The Assistant Secretary may designate under paragraph (1) a position filled by an employee who was employed in that position on the day before the date of the enactment of this Act only if the employee was in the top one-third of performance rankings for the position within the Office for the duration of the 2-year period ending on the date of the enactment of this Act.

(e) BRIEFING ON THE PILOT PROGRAM.—Not later than 180 days after the date of the enactment of this Act and not less frequently than once each year thereafter for the duration of the period set forth in subsection (b), the Assistant Secretary shall provide the congressional intelligence committees and the Director of National Intelligence with a briefing on the pilot program required by subsection (a).

(f) REPORT ON THE PILOT PROGRAM.—Not later than 180 days before the last day of the period set forth in subsection (b), the Assistant Secretary shall submit to the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the

House of Representatives, and the Director of National Intelligence a report on the effectiveness of the pilot program and recommendations on whether the pilot program should be extended, modified, or ended.

(g) RECOMMENDATIONS OF DIRECTOR OF NATIONAL INTELLIGENCE.—Not later than 3 years after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees recommendations as to—

(1) which, if any, other elements of the intelligence community would benefit from a program similar to the pilot program required by subsection (a); and

(2) what, if any, modifications the Director would recommend for such elements.

(h) RETENTION OF PRESCRIBED RATES OF PAY AFTER TERMINATION OF PILOT PROGRAM.—After the period set forth in subsection (b), the Assistant Secretary may continue to pay a person, who received pay during such period pursuant to a rate of basic pay prescribed under subsection (c), at a rate of basic pay not to exceed the rate of basic pay that was in effect for the person on the day before the last day of such period, until such time as the applicable rate of basic pay for the person under

the General Schedule exceeds the rate of basic pay that was so in effect under subsection (c).

SEC. 315. PILOT PROGRAM ON STUDENT LOAN REPAYMENT AT OFFICE OF INTELLIGENCE AND ANALYSIS OF DEPARTMENT OF THE TREASURY.

(a) PILOT PROGRAM.—

(1) ESTABLISHMENT.—The Assistant Secretary for Intelligence and Analysis in the Department of the Treasury shall carry out a pilot program to assess the feasibility and advisability of using repayment of loans on behalf of persons that were used by the persons to finance education as a recruitment incentive for employment at the Office of Intelligence and Analysis of China specialists, data scientists, cyber specialists, and others with any other analytic or technical capabilities that are in high demand by the Office.

(b) LOAN REPAYMENTS.—

(1) IN GENERAL.—Under the pilot program, the Assistant Secretary may repay the principal, interest, and related expenses of a loan obtained by a covered person to finance education.

(2) COVERED PERSONS.—For purposes of paragraph (1), a covered person is a person who agrees to an offer from the Assistant Secretary to partici-

pate in the pilot program before beginning employment in the Office.

(3) LIMITATION ON TOTAL AMOUNT.—Under the pilot program, the Assistant Secretary may repay not more than $100,000 on behalf of any one person.

(4) LIMITATION ON ANNUAL AMOUNT OF PAYMENTS.—Under the pilot program, the Assistant Secretary may repay not more than $15,000 on behalf of any one person in any one fiscal year.

(5) TIMING AND PERIOD OF PAYMENTS.—In repaying a loan of a person under the pilot program, the Assistant Secretary shall make payments—

(A) on a monthly basis; and

(B) only during the period beginning on the date on which the person begins employment with the Office and ending on the date on which the person leaves employment with the Office.

(c) DURATION.—The Assistant Secretary shall carry out the pilot program during the period of fiscal years 2022 through 2024.

(d) LIMITATION ON NUMBER OF PARTICIPANTS.—The total number of individuals receiving a loan repay-

ment under the pilot program during any fiscal year may not exceed 10.

(e) ADMINISTRATION.—

(1) IN GENERAL.—In carrying out the pilot program, the Assistant Secretary shall—

(A) establish such requirements relating to the academic or specialized training of participants as the Assistant Secretary considers appropriate to ensure that participants are prepared for employment as intelligence analysts; and

(B) periodically review the areas of high demand for particular analytic or technical capabilities and determine which academic areas of specialization may be most useful in addressing that demand.

(2) USE OF EXISTING PROGRAMS.—The Assistant Secretary shall assess the feasibility and advisability of administering the pilot program by leveraging student loan programs of the Department of the Treasury that were in effect on the day before the date of the enactment of this Act.

(f) REPORTS.—

(1) PRELIMINARY REPORT.—Not later than 120 days after the date of the enactment of this Act,

the Assistant Secretary shall submit to Congress a preliminary report on the pilot program, including a description of the pilot program and the authorities to be utilized in carrying out the pilot program.

(2) ANNUAL REPORT.—

(A) IN GENERAL.—Not later than one year after the commencement of the pilot program and annually thereafter until the program ends, the Assistant Secretary shall submit to the congressional intelligence committees and the Director of National Intelligence a report on the pilot program.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall include—

(i) a description of the activities under the pilot program, including the number of individuals who participated in the pilot program;

(ii) an assessment of the effectiveness of the pilot program as a recruitment tool; and

(iii) such recommendations for legislative or administrative action as the Assistant Secretary considers appropriate in light of the pilot program.

(3) RECOMMENDATIONS.—Not later than 2 years after the commencement of the pilot program, the Director of National Intelligence shall submit to the congressional intelligence committees the recommendations of the Director as to which, if any, other elements of the intelligence community would benefit from establishing a loan repayment program similar to the pilot program required by subsection (a), and what, if any, modifications the Director would recommend to the program if it were established.

(g) FUNDING.—Of the amounts authorized to be appropriated by this Act, $1,300,000 shall be available until expended to carry out this section. Of such amounts—

(1) $1,000,000 shall be available for repayment of loans; and

(2) $300,000 shall be available for a period of 2 years during the pilot program to hire personnel to administer the pilot program.

SEC. 316. PROHIBITION ON COLLECTION AND ANALYSIS OF UNITED STATES PERSONS' INFORMATION BY INTELLIGENCE COMMUNITY BASED ON FIRST AMENDMENT-PROTECTED ACTIVITIES.

No element of the intelligence community may collect or analyze a United States person's information solely

upon the basis of an activity protected by the First Amendment to the Constitution of the United States.

SEC. 317. SENSE OF THE SENATE ON THE USE OF INTELLIGENCE COMMUNITY RESOURCES FOR COLLECTION, ASSESSMENT, AND ANALYSIS OF INFORMATION PERTAINING EXCLUSIVELY TO UNITED STATES PERSONS ABSENT A FOREIGN NEXUS.

It is the sense of the Senate that—

(1) the Federal Bureau of Investigation and the Department of Homeland Security do vital work in enforcing the rule of law and safeguarding the people of the United States from harm;

(2) the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 118 Stat. 3638) sought to facilitate greater information sharing between law enforcement and intelligence communities for the purpose of thwarting attacks on the homeland from international terrorist organizations;

(3) National Intelligence Program funds should be expended only in support of intelligence activities with a foreign nexus consistent with the definition of intelligence provided by Congress in section 3 of the

National Security Act of 1947 (50 U.S.C. 3003); and

(4) the intelligence community should not engage in the collection, assessment, or analysis of information that pertains exclusively to United States persons absent a foreign nexus.

Subtitle B—Inspector General of the Intelligence Community

SEC. 321. SUBMITTAL OF COMPLAINTS AND INFORMATION BY WHISTLEBLOWERS IN THE INTELLIGENCE COMMUNITY TO CONGRESS.

(a) AMENDMENTS TO INSPECTOR GENERAL ACT OF 1978.—

(1) APPOINTMENT OF SECURITY OFFICERS.—Section 8H of the Inspector General Act of 1978 (5 U.S.C. App.) is amended—

(A) by redesignating subsection (h) as subsection (i); and

(B) by inserting after subsection (g) the following:

''(h) APPOINTMENT OF SECURITY OFFICERS.—Each Inspector General under this section, including the designees of the Inspector General of the Department of Defense pursuant to subsection (a)(3), shall appoint within their offices security officers to provide, on a permanent

basis, confidential, security-related guidance and direction to an employee of their respective establishment, an employee assigned or detailed to such establishment, or an employee of a contractor of such establishment who intends to report to Congress a complaint or information, so that such employee can obtain direction on how to report to Congress in accordance with appropriate security practices.''.

(2) PROCEDURES.—Subsection (d) of such section is amended—

(A) by amending paragraph (2) to read as follows:

''(2)(A) Except as provided in subparagraph (B), the employee may contact the intelligence committees directly as described in paragraph (1) of this subsection or in subsection (a)(4) only if the employee—

''(i) before making such a contact, furnishes to the head of the establishment, through the Inspector General (or designee), a statement of the employee's complaint or information and notice of the employee's intent to contact the intelligence committees directly; and

''(ii)(I) obtains and follows from the head of the establishment, through the Inspector General (or designee), procedural direction on how to contact the

intelligence committees in accordance with appropriate security practices; or

''(II) obtains and follows such procedural direction from the applicable security officer appointed under subsection (h).

''(B) If an employee seeks procedural direction under subparagraph (A)(ii) and does not receive such procedural direction within 30 days, or receives insufficient direction to report to Congress a complaint or information, the employee may contact the intelligence committees directly without obtaining or following the procedural direction otherwise required under such subparagraph.''; and

(B) by redesignating paragraph (3) as paragraph (4); and

(C) by inserting after paragraph (2) the following:

''(3) An employee of an element of the intelligence community who intends to report to Congress a complaint or information may report such complaint or information to—

''(A) the Chairman and Vice Chairman of the Select Committee on Intelligence of the Senate, a nonpartisan member of the committee staff designated for purposes of receiving complaints or information under this section, or a member of the

majority staff and a member of the minority staff of the committee; or

''(B) the Chairman and Ranking Member of the Permanent Select Committee on Intelligence of the House of Representatives, a nonpartisan member of the committee staff designated for purposes of receiving complaints or information under this section, or a member of the majority staff and a member of the minority staff of the committee.''.

(3) CLARIFICATION OF RIGHT TO REPORT DIRECTLY TO CONGRESS.—Subsection (a) of such section is amended by adding at the end the following:

''(4) Subject to paragraphs (2) and (3) of subsection (d), an employee of an element of the intelligence community who intends to report to Congress a complaint or information may report such complaint or information directly to Congress, regardless of whether the complaint or information is with respect to an urgent concern—

''(A) in lieu of reporting such complaint or information under paragraph (1); or

''(B) in addition to reporting such complaint or information under paragraph (1).''.

(b) AMENDMENTS TO NATIONAL SECURITY ACT OF 1947.—

(1) APPOINTMENT OF SECURITY OFFICERS.—Section 103H(j) of the National Security Act of 1947 (50 U.S.C. 3033(j)) is amended by adding at the end the following:

''(5) The Inspector General shall appoint within the Office of the Inspector General security officers as required by subsection (h) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.).''.

(2) PROCEDURES.—Subparagraph (D) of section 103H(k)(5) of such Act (50 U.S.C. 3033(k)(5)) is amended—

(A) by amending clause (ii) to read as follows:

''(ii)(I) Except as provided in subclause (II), an employee may contact the congressional intelligence committees directly as described in clause (i) only if the employee—

''(aa) before making such a contact, furnishes to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the congressional intelligence committees directly; and

''(bb)(AA) obtains and follows from the Director, through the Inspector General, procedural direc-

tion on how to contact the intelligence committees in accordance with appropriate security practices; or

''(BB) obtains and follows such procedural direction from the applicable security officer appointed under section 8H(h) of the Inspector General Act of 1978 (5 U.S.C. App.).

''(II) If an employee seeks procedural direction under subclause (I)(bb) and does not receive such procedural direction within 30 days, or receives insufficient direction to report to Congress a complaint or information, the employee may contact the congressional intelligence committees directly without obtaining or following the procedural direction otherwise required under such subclause.'';

(B) by redesignating clause (iii) as clause (iv); and

(C) by inserting after clause (ii) the following:

''(iii) An employee of an element of the intelligence community who intends to report to Congress a complaint or information may report such complaint or information to—

''(I) the Chairman and Vice Chairman of the Select Committee on Intelligence of the Senate, a nonpartisan member of the committee staff designated for purposes of receiving complaints or in-

formation under this section, or a member of the majority staff and a member of the minority staff of the committee; or

''(II) the Chairman and Ranking Member of the Permanent Select Committee on Intelligence of the House of Representatives, a nonpartisan member of the committee staff designated for purposes of receiving complaints or information under this section, or a member of the majority staff and a member of the minority staff of the committee.''.

(3) CLARIFICATION OF RIGHT TO REPORT DIRECTLY TO CONGRESS.—Subparagraph (A) of such section is amended—

(A) by inserting ''(i)'' before ''An employee of''; and

(B) by adding at the end the following:

''(ii) Subject to clauses (ii) and (iii) of subparagraph (D), an employee of an element of the intelligence community who intends to report to Congress a complaint or information may report such complaint or information directly to Congress, regardless of whether the complaint or information is with respect to an urgent concern—

''(A) in lieu of reporting such complaint or information under clause (i); or

''(B) in addition to reporting such complaint or information under clause (i).''.

(c) AMENDMENTS TO THE CENTRAL INTELLIGENCE AGENCY ACT OF 1949.—

(1) APPOINTMENT OF SECURITY OFFICERS.—Section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)) is amended by adding at the end the following:

''(I) The Inspector General shall appoint within the Office of the Inspector General security officers as required by subsection (h) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.).''.

(2) PROCEDURES.—Subparagraph (D) of such section is amended—

(A) by amending clause (ii) to read as follows:

''(ii)(I) Except as provided in subclause (II), an employee may contact the intelligence committees directly as described in clause (i) only if the employee—

''(aa) before making such a contact, furnishes to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the intelligence committees directly; and

''(bb)(AA) obtains and follows from the Director, through the Inspector General, procedural direction on how to contact the intelligence committees in accordance with appropriate security practices; or

''(BB) obtains and follows such procedural direction from the applicable security officer appointed under section 8H(h) of the Inspector General Act of 1978 (5 U.S.C. App.).

''(II) If an employee seeks procedural direction under subclause (I)(bb) and does not receive such procedural direction within 30 days, or receives insufficient direction to report to Congress a complaint or information, the employee may contact the congressional intelligence committees directly without obtaining or following the procedural direction otherwise required under such subclause.'';

(B) by redesignating clause (iii) as clause (iv); and

(C) by inserting after clause (ii) the following:

''(iii) An employee of the Agency who intends to report to Congress a complaint or information may report such complaint or information to—

''(I) the Chairman and Vice Chairman of the Select Committee on Intelligence of the Senate, a nonpartisan member of the committee staff des-

ignated for purposes of receiving complaints or information under this section, or a member of the majority staff and a member of the minority staff of the committee; or

''(II) the Chairman and Ranking Member of the Permanent Select Committee on Intelligence of the House of Representatives, a nonpartisan member of the committee staff designated for purposes of receiving complaints or information under this section, or a member of the majority staff and a member of the minority staff of the committee.''.

(3) CLARIFICATION OF RIGHT TO REPORT DIRECTLY TO CONGRESS.—Subparagraph (A) of such section is amended—

(A) by inserting ''(i)'' before ''An employee of''; and

(B) by adding at the end the following:

''(ii) Subject to clauses (ii) and (iii) of subparagraph (D), an employee of the Agency who intends to report to Congress a complaint or information may report such complaint or information directly to Congress, regardless of whether the complaint or information is with respect to an urgent concern—

''(A) in lieu of reporting such complaint or information under clause (i); or

''(B) in addition to reporting such complaint or information under clause (i).''.

SEC. 322. DEFINITIONS AND AUTHORITIES REGARDING WHISTLEBLOWER COMPLAINTS AND INFORMATION OF URGENT CONCERN RECEIVED BY INSPECTORS GENERAL OF THE INTELLIGENCE COMMUNITY.

(a) DEFINITION OF URGENT CONCERN.—

(1) NATIONAL SECURITY ACT OF 1947.—Section 103H(k)(5)(G)(i) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)(G)(i)) is amended by striking ''within the'' and all that follows through ''policy matters.'' and inserting the following: ''of the Federal Government that is—

''(I) a matter of national security; and

''(II) not a difference of opinion concerning public policy matters.''.

(2) INSPECTOR GENERAL ACT OF 1978.—Paragraph (1)(A) of subsection (i) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.), as redesignated by section 321(a)(1)(A), is amended by striking ''involving'' and all that follows through ''policy matters.'' and inserting the following: ''of the Federal Government that is—

''(i) a matter of national security; and

''(ii) not a difference of opinion concerning public policy matters.''.

(3) CENTRAL INTELLIGENCE AGENCY ACT OF 1949.—Section 17(d)(5)(G)(i)(I) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)(G)(i)(I)) is amended by striking ''involving'' and all that follows through ''policy matters.'' and inserting the following: ''of the Federal Government that is—

''(aa) a matter of national security; and

''(bb) not a difference of opinion concerning public policy matters.''.

(b) AUTHORITY OF INSPECTORS GENERAL.—

(1) SCOPE OF AUTHORITY OF INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.—Section 103H(k)(5) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)) is amended by adding at the end the following:

''(J) The Inspector General shall have authority over any complaint or information submitted to the Inspector General from an employee, detailee, or contractor, or former employee, detailee, or contractor, of the intelligence community.''.

(2) AUTHORITY OF INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY TO DETERMINE MATTERS OF URGENT CONCERN.—Section 103H(k)(5)(G) of such Act (50 U.S.C. 3033(k)(5)(G)) is amended—

(A) in clause (i), as amended by subsection (a)(1), by resdesignating subclauses (I) and (II) as items (aa) and (bb), respectively;

(B) by redesignating clauses (i), (ii), and (iii) as subclauses (I), (II), and (III), respectively;

(C) in the matter before subclause (I), as redesignated by subparagraph (B), by inserting ''(i)'' before ''In this''; and

(D) by adding at the end the following:

''(ii) The Inspector General shall have sole authority to determine whether any complaint or information reported to the Inspector General is a matter of urgent concern under this paragraph.''.

(3) AUTHORITY OF INSPECTORS GENERAL TO DETERMINE MATTERS OF URGENT CONCERN.—Subsection (i) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.), as redesignated by section 321(a)(1)(A), is amended—

(A) in paragraph (1)—

(i) in subparagraph (A), as amended by subsection (a)(2), by redesignating clauses (i) and (ii) as subclauses (I) and (II), respectively; and

(ii) by redesignating paragraphs (A), (B), and (C) and clauses (i), (ii), and (iii), respectively;

(B) by redesignating paragraphs (1) and (2) as subparagraphs (A) and (B), respectively;

(C) in the matter before subparagraph (A), as redesignated by subparagraph (B), by inserting ''(1)'' before ''In this''; and

(D) by adding at the end the following:

''(2) The Inspector General shall have sole authority to determine whether any complaint or information reported to the Inspector General is a matter of urgent concern under this section.''.

(4) AUTHORITY OF INSPECTOR GENERAL OF CENTRAL INTELLIGENCE AGENCY TO DETERMINE MATTERS OF URGENT CONCERN.—Section 17(d)(5)(G) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)(G)) is amended—

(A) in clause (i)—

(i) in subclause (I), as amended by subsection (a)(3), by redesignating items

(aa) and (bb) as subitems (AA) and (BB), respectively; and

(ii) by redesignating subclauses (I), (II), and (III) as items (aa), (bb), and (cc), respectively;

(B) by redesignating clauses (i) and (ii) as subclauses (I) and (II), respectively; and

(C) in the matter before clause (I), as redesignated by subparagraph (B), by inserting ''(i)'' before ''In this''; and

(D) by adding at the end the following:

''(ii) The Inspector General shall have sole authority to determine whether any complaint or information reported to the Inspector General is a matter of urgent concern under this paragraph.''.

SEC. 323. HARMONIZATION OF WHISTLEBLOWER PROTECTIONS.

(a) PROHIBITED PERSONNEL PRACTICES IN THE INTELLIGENCE COMMUNITY.—

(1) THREATS RELATING TO PERSONNEL ACTIONS.—

(A) AGENCY EMPLOYEES.—Section 1104(b) of the National Security Act of 1947 (50 U.S.C. 3234(b)) is amended, in the matter preceding paragraph (1), by inserting '', or

threaten to take or fail to take,'' after ''take or fail to take''.

(B) CONTRACTOR EMPLOYEES.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1)) is amended, in the matter preceding subparagraph (A), by inserting '', or threaten to take or fail to take,'' after ''take or fail to take''.

(2) PROTECTION FOR CONTRACTOR EMPLOYEES AGAINST REPRISAL FROM AGENCY EMPLOYEES.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1)), as amended by paragraph (1)(B) of this subsection, is further amended, in the matter preceding subparagraph (A), by inserting ''of an agency or'' after ''Any employee''.

(3) ENFORCEMENT.—Subsection (d) of section 1104 of such Act (50 U.S.C. 3234) is amended to read as follows:

''(d) ENFORCEMENT.—The President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.''.

(b) RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.—

(1) ENFORCEMENT.—Section 3001(j) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)) is amended—

(A) by redesignating paragraph (8) as paragraph (9); and

(B) by inserting after paragraph (7) the following:

''(8) ENFORCEMENT.—Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.''.

(2) ELIMINATION OF DEADLINE FOR APPEAL OF PROHIBITED REPRISAL.—Section 3001(j)(4)(A) of such Act (50 U.S.C. 3341(j)(4)(A)) is amended by striking ''within 90 days''.

(3) ELIMINATION OF CAP ON COMPENSATORY DAMAGES.—Section 3001(j)(4)(B) of such Act (50 U.S.C. 3341(j)(4)(B)) is amended, in the second sentence, by striking ''not to exceed $300,000''.

(4) ESTABLISHING PROCESS PARITY FOR ADVERSE SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—Subparagraph (C) of section

3001(j)(4) of such Act (50 U.S.C. 3341(j)(4)) is amended to read as follows:

"(C) BURDENS OF PROOF.—

"(i) IN GENERAL.—Subject to clause (iii), in determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall find that paragraph (1) was violated if the individual has demonstrated that a disclosure described in paragraph (1) was a contributing factor in the adverse security clearance or access determination taken against the individual.

"(ii) CIRCUMSTANTIAL EVIDENCE.—An individual under clause (i) may demonstrate that the disclosure was a contributing factor in the adverse security clearance or access determination taken against the individual through circumstantial evidence, such as evidence that—

"(I) the official making the determination knew of the disclosure; and

"(II) the determination occurred within a period such that a reasonable

person could conclude that the disclosure was a contributing factor in the determination.

''(iii) DEFENSE.—In determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall not find that paragraph (1) was violated if, after a finding that a disclosure was a contributing factor, the agency demonstrates by clear and convincing evidence that it would have made the same security clearance or access determination in the absence of such disclosure.''.

(c) CORRECTION OF DEFINITION OF AGENCY.—Section 3001(a)(1)(B) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(a)(1)(B)) is amended by striking ''and'' and inserting ''or''.

(d) ESTABLISHING CONSISTENCY WITH RESPECT TO PROTECTIONS FOR DISCLOSURES OF MISMANAGEMENT.—

(1) SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—Section 3001(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)) is amended—

(A) in subparagraph (A)(ii), by striking ''gross mismanagement'' and inserting ''mismanagement''; and

(B) in subparagraph (B)(ii), by striking ''gross mismanagement'' and inserting ''mismanagement''.

(2) PERSONNEL ACTIONS AGAINST CONTRACTOR EMPLOYEES.—Section 1104(c)(1)(B) of the National Security Act of 1947 (50 U.S.C. 3234(c)(1)(B)) is amended by striking ''gross mismanagement'' and inserting ''mismanagement''.

(e) PROTECTED DISCLOSURES TO SUPERVISORS.—

(1) PERSONNEL ACTIONS.—

(A) DISCLOSURES BY AGENCY EMPLOYEES TO SUPERVISORS.—Section 1104(b) of the National Security Act of 1947 (50 U.S.C. 3234(b)), as amended by subsection (a)(1)(A), is further amended, in the matter preceding paragraph (1), by inserting ''a supervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including'' before ''the head of the employing agency''.

(B) DISCLOSURES BY CONTRACTOR EMPLOYEES TO SUPERVISORS.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1)), as amended by subsection (a), is further amended, in the matter preceding subparagraph (A), by inserting ''a supervisor in the contractor employee's direct chain of command up to and including'' before ''the head of the contracting agency''.

(2) SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—Section 3001(j)(1)(A) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)(A)) is amended, in the matter preceding clause (i), by inserting ''a supervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including'' before ''the head of the employing agency''.

(f) ESTABLISHING PARITY FOR PROTECTED DISCLOSURES.—Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is amended—

(1) in subsection (b), as amended by subsections (a)(1)(A) and (e)(1)(A)—

(A) by redesignating paragraphs (1) and (2) as subparagraphs (A) and (B), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the right;

(B) in the matter preceding subparagraph (A), as redesignated and moved by subparagraph (B) of this paragraph, by striking ''for a lawful disclosure'' and inserting the following: ''for—

''(1) any lawful disclosure''; and

(C) by adding at the end the following:

''(2) any lawful disclosure that complies with—

''(A) subsections (a)(1), (d), and (g) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);

''(B) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or

''(C) subparagraphs (A), (D), and (I) of section 103H(k)(5); or

''(3) if the actions do not result in the employee unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

''(A) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

''(B) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in subparagraph (A); or

''(C) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.''; and

(2) in subsection (c)(1), as amended by subsections (a) and (e)(1)(B)—

(A) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively, and moving such clauses, as so redesignated, 2 ems to the right;

(B) in the matter preceding clause (i), as redesignated and moved by subparagraph (B) of this paragraph, by striking ''for a lawful disclosure'' and inserting the following: ''for—

''(A) any lawful disclosure''; and

(C) by adding at the end the following:

''(B) any lawful disclosure that complies with—

"(i) subsections (a)(1), (d), and (g) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);

"(ii) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or

"(iii) subparagraphs (A), (D), and (I) of section 103H(k)(5); or

"(C) if the actions do not result in the contractor employee unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

"(i) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

"(ii) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in clause (i); or

"(iii) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or in-

vestigation conducted by the Inspector General.''.

(g) CLARIFICATION RELATING TO PROTECTED DISCLOSURES.—Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is amended—

(1) by redesignating subsections (d) and (e) as subsections (f) and (g), respectively; and

(2) by inserting after subsection (c) the following:

''(d) RULE OF CONSTRUCTION.—Consistent with the protection of sources and methods, nothing in subsection (b) or (c) shall be construed to authorize—

''(1) the withholding of information from Congress; or

''(2) the taking of any personnel action against an employee who lawfully discloses information to Congress.

''(e) DISCLOSURES.—A disclosure shall not be excluded from this section because—

''(1) the disclosure was made to an individual, including a supervisor, who participated in an activity that the employee reasonably believed to be covered under subsection (b)(1)(B) or the contractor employee reasonably believed to be covered under subsection (c)(1)(A)(ii);

"(2) the disclosure revealed information that had been previously disclosed;

"(3) the disclosure was not made in writing;

"(4) the disclosure was made while the employee was off duty;

"(5) of the amount of time which has passed since the occurrence of the events described in the disclosure; or

"(6) the disclosure was made during the normal course of duties of an employee or contractor employee.".

(h) CORRECTION RELATING TO NORMAL COURSE DISCLOSURES.—Section 3001(j)(3) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(3)) is amended—

(1) by striking "DISCLOSURES.—" and all that follows through "because—" and inserting "DISCLOSURES.—A disclosure shall not be excluded from paragraph (1) because—";

(2) by striking subparagraph (B);

(3) by redesignating clauses (i) through (v) as subparagraphs (A) through (E), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the left;

(4) in subparagraph (D), as so redesignated, by striking ''or'' at the end;

(5) in subparagraph (E), as redesignated by paragraph (3), by striking the period at the end and inserting ''; or''; and

(6) by adding at the end the following:

''(F) the disclosure was made during the normal course of duties of an employee.''.

(i) CLARIFICATION RELATING TO RULE OF CONSTRUCTION.—Section 3001(j)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(2)) is amended by inserting ''or clearance action'' after ''personnel action''.

(j) CLARIFICATION RELATING TO PROHIBITED PRACTICES.—

(1) INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004.—Section 3001(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)), as amended by this section, is further amended by striking ''over'' and inserting ''to take, materially impact, direct others to take, recommend, or approve''.

(2) NATIONAL SECURITY ACT OF 1947.—

(A) AGENCY EMPLOYEES.—Section 1104(b) of the National Security Act of 1947

(50 U.S.C. 3234(b)), as amended by this section, is further amended by inserting ''materially impact,'' after ''authority to take,''

(B) CONTRACTOR EMPLOYEES.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1)), as amended by this section, is further amended by inserting ''materially impact,'' after ''authority to take,''.

(k) TECHNICAL CORRECTION.—Section 3001(j)(1)(C)(i) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)(C)(i)) is amended by striking ''(h)'' and inserting ''(g)''.

(l) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community shall submit to the congressional intelligence committees a report assessing the extent to which protections provided under Presidential Policy Directive 19 (relating to protecting whistleblowers with access to classified information) have been codified in statutes.

SEC. 324. PROHIBITION AGAINST DISCLOSURE OF WHISTLEBLOWER IDENTITY AS REPRISAL AGAINST WHISTLEBLOWER DISCLOSURE BY EMPLOYEES AND CONTRACTORS IN INTELLIGENCE COMMUNITY.

(a) IN GENERAL.—Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is amended—

(1) in subsection (a)(3) of such section—

(A) in subparagraph (I), by striking ''; or'' and inserting a semicolon;

(B) by redesignating subparagraph (J) as subparagraph (K); and

(C) by inserting after subparagraph (I) the following:

''(J) a knowing and willful disclosure revealing the identity or other personally identifiable information of an employee or contractor employee; or'';

(2) by redesignating subsections (f) and (g), as redesignated by section 323(g)(1), as subsections (g) and (h), respectively; and

(3) by inserting after subsection (e), as added by section 323(g)(2), the following:

''(f) PERSONNEL ACTIONS INVOLVING DISCLOSURES OF WHISTLEBLOWER IDENTITY.—A personnel action described in subsection (a)(3)(J) shall not be considered in

violation of subsection (b) or (c) under the following circumstances:

"(1) The personnel action was taken with the express consent of the employee or contractor employee.

"(2) An Inspector General with oversight responsibility for a covered intelligence community element determines that—

"(A) the personnel action was unavoidable under section 103H(g)(3)(A) of this Act (50 U.S.C. 3033(g)(3)(A)), section 17(e)(3)(A) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(e)(3)(A)), or section 8M(b)(2)(B) of the Inspector General Act of 1978 (5 U.S.C. App.);

"(B) the personnel action was made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken; or

"(C) the personnel action was required by statute or an order from a court of competent jurisdiction.".

(b) APPLICABILITY TO DETAILEES.—Subsection (a) of section 1104 of such Act (50 U.S.C. 3234) is amended by adding at the end the following:

''(5) EMPLOYEE.—The term 'employee', with respect to an agency or a covered intelligence community element, includes an individual who has been detailed to such agency or covered intelligence community element.''.

(c) PRIVATE RIGHT OF ACTION FOR UNLAWFUL DISCLOSURE OF WHISTLEBLOWER IDENTITY.—Subsection (g) of such section, as amended by subsection (a)(3) of section 323(a)(3), redesignated by subsection (g)(1) of such section, and further redesignated by subsection (a)(2) of this section, is amended to read as follows:

''(g) ENFORCEMENT.—

''(1) IN GENERAL.—Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section.

''(2) HARMONIZATION WITH OTHER ENFORCEMENT.—To the fullest extent possible, the President shall provide for enforcement of this section in a manner that is consistent with the enforcement of section 2302(b)(8) of title 5, United States Code, especially with respect to policies and procedures used to adjudicate alleged violations of such section.

''(3) PRIVATE RIGHT OF ACTION FOR DISCLOSURES OF WHISTLEBLOWER IDENTITY IN VIOLATION OF PROHIBITION AGAINST REPRISALS.—Subject to

paragraph (4), in a case in which an employee of an agency takes a personnel action described in subsection (a)(3)(J) against an employee of a covered intelligence community element as a reprisal in violation of subsection (b) or in a case in which an employee or contractor employee takes a personnel action described in subsection (a)(3)(J) against another contractor employee as a reprisal in violation of subsection (c), the employee or contractor employee against whom the personnel action was taken may, consistent with section 1221 of title 5, United States Code, bring a private action for all appropriate remedies, including injunctive relief and compensatory and punitive damages, in an amount not to exceed $250,000, against the agency of the employee or contracting agency of the contractor employee who took the personnel action, in a Federal district court of competent jurisdiction.

''(4) REQUIREMENTS.—

''(A) REVIEW BY INSPECTOR GENERAL AND BY EXTERNAL REVIEW PANEL.—Before the employee or contractor employee may bring a private action under paragraph (3), the employee or contractor employee shall exhaust administrative remedies by—

''(i) first, obtaining a disposition of their claim by requesting review of the appropriate inspector general; and

''(ii) second, submitting to the Inspector General of the Intelligence Community a request for a review of the claim by an external review panel under section 1106.

''(B) PERIOD TO BRING ACTION.—The employee or contractor employee may bring a private right of action under paragraph (3) during the 180-day period beginning on the date on which the employee or contractor employee is notified of the final disposition of their claim under section 1106.''.

Subtitle C—Reports and Assessments Pertaining to the Intelligence Community

SEC. 331. REPORT ON EFFORTS TO BUILD AN INTEGRATED HYBRID SPACE ARCHITECTURE.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

(b) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, and annually for 2 years thereafter, the Director of National Intelligence, in coordination with the Under Secretary of Defense for Intelligence and Security and the Director of the National Reconnaissance Office, shall submit to the appropriate committees of Congress a report on the efforts of the intelligence community to build an integrated hybrid space architecture that combines national and commercial capabilities and large and small satellites.

(c) ELEMENTS.—The report required by subsection (b) shall include the following:

(1) An assessment of how the integrated hybrid space architecture approach is being realized in the overhead architecture of the National Reconnaissance Office.

(2) An assessment of the benefits to the mission of the National Reconnaissance Office and the cost of integrating capabilities from smaller, proliferated satellites and data from commercial satellites with the national technical means architecture.

SEC. 332. REPORT ON PROJECT MAVEN TRANSITION.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

(b) REPORT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Director of the National Geospatial-Intelligence Agency, in consultation with such other Federal Government entities as the Director considers appropriate, shall submit to the appropriate committees of Congress a report on the transition of Project Maven to operational mission support.

(c) PLAN OF ACTION AND MILESTONES.—The report required by subsection (b) shall include a detailed plan of action and milestones that identifies—

(1) the milestones and decision points leading up to the transition of successful geospatial intelligence capabilities developed under Project Maven to the National Geospatial-Intelligence Agency; and

(2) the metrics of success regarding the transition described in paragraph (1) and mission support

provided to the National Geospatial-Intelligence Agency for each of fiscal years 2022 and 2023.

(d) FORM.—The report required by subsection (b) shall be submitted in unclassified form, but may include a classified annex.

SEC. 333. ASSESSMENT OF INTELLIGENCE COMMUNITY COUNTERNARCOTICS CAPABILITIES.

(a) ASSESSMENT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with such other Federal Government entities as the Director considers appropriate, submit to the congressional intelligence committees an assessment on the status of the intelligence community's—

(1) counternarcotics capabilities and resourcing with regard to intelligence collection and analysis;

(2) operational support to foreign liaison partners; and

(3) operational capacity to support the counternarcotics mission of the Federal Government.

(b) FORM.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 334. ASSESSMENT OF INTELLIGENCE COMMUNITY'S INTELLIGENCE-SHARING RELATIONSHIPS WITH LATIN AMERICAN PARTNERS IN COUNTERNARCOTICS.

(a) ASSESSMENT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with such other Federal Government entities as the Director considers appropriate, submit to the congressional intelligence committees an assessment on the intelligence-sharing relationships of the intelligence community with foreign partners in Latin America on counternarcotics matters.

(b) FORM.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 335. REPORT ON UNITED STATES SOUTHERN COMMAND INTELLIGENCE CAPABILITIES.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

(b) REPORT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Director of the Defense Intelligence Agency, in consultation with such other Federal Government entities as the Director considers relevant, shall submit to the appropriate committees of Congress a report detailing the status of United States Southern Command's intelligence collection, analysis, and operational capabilities to support Latin America-based missions.

(c) FORM.—The report required by subsection (b) shall be submitted in unclassified form, but may include a classified annex.

SEC. 336. DIRECTOR OF NATIONAL INTELLIGENCE REPORT ON TRENDS IN TECHNOLOGIES OF STRATEGIC IMPORTANCE TO UNITED STATES.

(a) IN GENERAL.—Not less frequently than once every 2 years until the date that is 4 years after the date of the enactment of this Act, the Director of National Intelligence shall submit to Congress a report assessing commercial and foreign trends in technologies the Director considers of strategic importance to the national and economic security of the United States.

(b) CONTENTS.—The report required by subsection (a) shall include the following:

(1) A list of the top technology focus areas that the Director considers to be of the most strategic importance to the United States.

(2) A list of the top technology focus areas in which countries that are adversarial to the United States are poised to match or surpass the technological leadership of the United States.

(c) FORM.—Each report submitted under subsection (a) may take the form of a National Intelligence Estimate and shall be submitted in classified form, but may include an unclassified summary.

SEC. 337. REPORT ON NORD STREAM II COMPANIES AND INTELLIGENCE TIES.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services, the Committee on Energy and Commerce, the Com-

mittee on Financial Services, the Committee on Foreign Affairs, and the Committee on Appropriations of the House of Representatives.

(b) REPORT REQUIRED.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with other appropriate Federal Government entities, shall submit to the appropriate committees of Congress a report on Nord Stream II efforts, including:

(1) an unclassified list of all companies supporting the Nord Stream II project; and

(2) an updated assessment of current or former ties between Nord Stream's Chief Executive Officer and Russian, East German, or other hostile intelligence agencies.

(c) FORM.—The report required under subsection (b) shall be submitted in unclassified form, but may include a classified annex, if necessary.

SEC. 338. ASSESSMENT OF ORGANIZATION OF DEFENSIVE INNOVATION AND RESEARCH ACTIVITIES.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

(b) ASSESSMENT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with other appropriate Federal Government entities, shall submit to the appropriate committees of Congress an assessment of the activities and objectives of the Organization of Defensive Innovation and Research (SPND). This assessment shall include information about the composition of the organization, the relationship of its personnel to any research on weapons of mass destruction, and any sources of financial and material support that such organization receives, including from the Government of Iran.

(c) FORM.—The assessment required under subsection (b) shall be submitted in unclassified form, but may include a classified annex, if necessary.

SEC. 339. REPORT ON INTELLIGENCE COMMUNITY SUPPORT TO VISAS MANTIS PROGRAM.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Foreign Relations, the Committee on the Judiciary, and the Committee on Appropriations of the Senate; and

(3) the Committee on Foreign Affairs, the Committee on the Judiciary, and the Committee on Appropriations of the House of Representatives.

(b) REPORT.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the head of any other appropriate Government entity, shall submit to the appropriate committees of Congress a report on intelligence matters relating to the Visas Mantis program, including efforts by—

(A) the intelligence community to provide and plan for effective intelligence support to such program; and

(B) hostile intelligence services to exploit such program or any other program by which visas for admission to the United States are issued.

(2) FORM.—The report required by paragraph (1) shall be submitted in unclassified form but may include a classified annex, as necessary.

SEC. 340. PLAN FOR ARTIFICIAL INTELLIGENCE DIGITAL ECOSYSTEM.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence shall—

(1) develop a plan for the development and resourcing of a modern digital ecosystem that embraces state-of-the-art tools and modern processes to enable development, testing, fielding, and continuous updating of artificial intelligence-powered applications at speed and scale from headquarters to the tactical edge; and

(2) submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives the plan developed under paragraph (1).

(b) CONTENTS OF PLAN.—At a minimum, the plan required by subsection (a) shall include the following:

(1) A roadmap for adopting a hoteling model to allow trusted small- and medium-sized artificial intelligence companies access to classified facilities on a flexible basis.

(2) An open architecture and an evolving reference design and guidance for needed technical investments in the proposed ecosystem that address issues, including common interfaces, authentication,

applications, platforms, software, hardware, and data infrastructure.

(3) A governance structure, together with associated policies and guidance, to drive the implementation of the reference throughout the intelligence community on a federated basis.

(4) Recommendations to ensure that use of artificial intelligence and associated data in Federal Government operations comport with rights relating to freedom of expression, equal protection, privacy, and due process.

(c) FORM.—The plan submitted under subsection (a)(2) shall be submitted in unclassified form, but may include a classified annex.

SEC. 341. STUDY ON UTILITY OF EXPANDED PERSONNEL MANAGEMENT AUTHORITY.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services of the Senate; and

(3) the Committee on Armed Services of the House of Representatives.

(b) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary of Defense for Intelligence and Security and the Director of National Intelligence shall jointly submit to the appropriate committees of Congress a study on the utility of providing elements of the intelligence community of the Department of Defense, other than the National Geospatial-Intelligence Agency, personnel management authority to attract experts in science and engineering under section 1599h of title 10, United States Code.

SEC. 342. ASSESSMENT OF ROLE OF FOREIGN GROUPS IN DOMESTIC VIOLENT EXTREMISM.

(a) ASSESSMENT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall—

(1) complete an assessment to identify the role of foreign groups, including entities, adversaries, governments, or other groups, in domestic violent extremist activities in the United States; and

(2) submit to the congressional intelligence committees the findings of the assessment completed under paragraph (1).

(b) FORM.—The findings submitted under subsection (a)(2) shall be submitted in unclassified form, but may include a classified annex.

SEC. 343. REPORT ON THE ASSESSMENT OF ALL-SOURCE CYBER INTELLIGENCE INFORMATION, WITH AN EMPHASIS ON SUPPLY CHAIN RISKS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the potential to strengthen all-source intelligence integration relating to foreign cyber threats, with an emphasis on cyber supply chain risks.

(b) CONTENTS.—The report required under subsection (a) shall include the following:

(1) An assessment of the effectiveness of the all-source cyber intelligence integration capabilities of the Office of the Director of National Intelligence and recommendations for such changes as the Director considers necessary to strengthen those capabilities.

(2) An assessment of the effectiveness of the Office of the Director of National Intelligence in analyzing and reporting on cyber supply chain risks, including efforts undertaken by the National Counterintelligence and Security Center.

(3) Mitigation plans for any gaps or deficiencies identified in the assessments included under paragraphs (1) and (2).

SEC. 344. REVIEW OF NATIONAL SECURITY AGENCY AND UNITED STATES CYBER COMMAND.

(a) REVIEW REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community and the Inspector General of the Department of Defense shall jointly complete a review of the National Security Agency and the United States Cyber Command.

(b) ELEMENTS.—The review required by subsection (a) shall include assessment of the following:

(1) Whether resources, authorities, activities, missions, facilities, and personnel are appropriately being delineated and used to conduct the intelligence and cybersecurity missions at the National Security Agency as well as the cyber offense and defense missions of United States Cyber Command.

(2) The extent to which current resource-sharing arrangements between the National Security Agency and United States Cyber Command lead to conflicts of interest in directing intelligence collection in support of United States Cyber Command missions rather than foreign intelligence collection.

(3) The intelligence analysis and production conducted by United States Cyber Command using National Security Agency authorities, with a focus

on analytic integrity and intelligence oversight to ensure proper analysis is informing mission operations.

(c) REPORT AND BRIEF.—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community and the Inspector General of the Department of Defense shall jointly submit to the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) a report and provide such committees a briefing on the findings of the inspectors general with respect to the review completed under subsection (a).

SEC. 345. SUPPORT FOR AND OVERSIGHT OF UNIDENTIFIED AERIAL PHENOMENA TASK FORCE.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' includes:

(A) The congressional intelligence committees.

(B) The Committee on Armed Services of the Senate.

(C) The Committee on Armed Services of the House of Representatives.

(2) UNIDENTIFIED AERIAL PHENOMENA TASK FORCE.—The term ''Unidentified Aerial Phenomena Task Force'' means the task force established by the Department of Defense on August 4, 2020, to be led by the Department of the Navy, under the Office of the Under Secretary of Defense for Intelligence and Security.

(b) AVAILABILITY OF DATA ON UNIDENTIFIED AERIAL PHENOMENA.—The Director of National Intelligence and the Secretary of Defense shall each, in coordination with each other, require each element of the intelligence community and the Department of Defense with data relating to unidentified aerial phenomena to make such data available immediately to the Unidentified Aerial Phenomena Task Force and to the National Air and Space Intelligence Center.

(c) QUARTERLY REPORTS TO CONGRESS.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act and not less frequently than quarterly thereafter, the Unidentified Aerial Phenomena Task Force, or such other entity as the Deputy Secretary of Defense may designate to be responsible for matters relating to unidentified aerial phenomena, shall submit to the appropriate committees of Congress quarterly reports

on the findings of the Unidentified Aerial Phenomena Task Force, or such other designated entity as the case may be.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include, at a minimum, the following:

(A) All reported unidentified aerial phenomena-related events that occurred during the previous 90 days.

(B) All reported unidentified aerial phenomena-related events that occurred during a time period other than the previous 90 days but were not included in an earlier report.

(3) FORM.—Each report submitted under paragraph (1) shall be submitted in classified form.

SEC. 346. PUBLICATION OF UNCLASSIFIED APPENDICES FROM REPORTS ON INTELLIGENCE COMMUNITY PARTICIPATION IN VULNERABILITIES EQUITIES PROCESS.

Section 6720(c) of the National Defense Authorization Act for Fiscal Year 2020 (50 U.S.C. 3316a(c)) is amended by adding at the end the following:

''(4) PUBLICATION.—The Director of National Intelligence shall make available to the public each

unclassified appendix submitted with a report under paragraph (1) pursuant to paragraph (2).''.

SEC. 347. REPORT ON FUTURE STRUCTURE AND RESPONSIBILITIES OF FOREIGN MALIGN INFLUENCE CENTER.

(a) ASSESSMENT AND REPORT REQUIRED.—Not later than one year after the date of the enactment of this Act, the Director of National Intelligence shall—

(1) conduct an assessment as to the future structure and responsibilities of the Foreign Malign Influence Center; and

(2) submit to the congressional intelligence committees a report on the findings of the Director with respect to the assessment conducted under paragraph (1).

(b) ELEMENTS.—The assessment conducted under subsection (a)(1) shall include an assessment of whether—

(1) the Director of the Foreign Malign Influence Center should continue to report directly to the Director of National Intelligence; or

(2) the Foreign Malign Influence Center should become an element of the National Counterintelligence and Security Center and the Director of the Foreign Malign Influence Center should report to

the Director of the National Counterintelligence and Security Center.

Subtitle D—People's Republic of China

SEC. 351. ASSESSMENT OF POSTURE AND CAPABILITIES OF INTELLIGENCE COMMUNITY WITH RESPECT TO ACTIONS OF THE PEOPLE'S REPUBLIC OF CHINA TARGETING TAIWAN.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

(b) ASSESSMENT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence and the Director of the Central Intelligence Agency shall jointly—

(1) complete an assessment to identify whether the posture and capabilities of the intelligence community are adequate to provide—

(A) sufficient indications and warnings regarding actions of the People's Republic of China targeting Taiwan; and

(B) policymakers with sufficient lead time to respond to actions described in subparagraph (A); and

(2) submit to the appropriate committees of Congress the findings of the assessment completed under paragraph (1).

(c) FORM.—The findings submitted under subsection (b)(2) shall be submitted in unclassified form, but may include a classified annex.

SEC. 352. PLAN TO COOPERATE WITH INTELLIGENCE AGENCIES OF KEY DEMOCRATIC COUNTRIES REGARDING TECHNOLOGICAL COMPETITION WITH PEOPLE'S REPUBLIC OF CHINA.

Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a plan to increase cooperation with the intelligence agencies of key democratic countries and key partners and allies of the United States in order to track and analyze the following:

(1) Technology capabilities and gaps among allied and partner countries of the United States.

(2) Current capabilities of the People's Republic of China in critical technologies and components.

(3) The efforts of the People's Republic of China to buy startups, conduct joint ventures, and invest in specific technologies globally.

(4) The technology development of the People's Republic of China in key technology sectors.

(5) The efforts of the People's Republic of China relating to standard-setting forums.

(6) Supply chain vulnerabilities for key technology sectors.

SEC. 353. ASSESSMENT OF PEOPLE'S REPUBLIC OF CHINA GENOMIC COLLECTION.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services, the Committee on Health, Education, Labor, and Pensions, and the Committee on Foreign Relations of the Senate; and

(3) the Committee on Armed Services, the Committee on Labor and Education, and the Committee on Foreign Affairs of the House of Representatives.

(b) ASSESSMENT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with other appropriate Federal Government entities, shall submit to the appropriate committees of Congress an assessment of the People's Republic of China's plans, intentions, capabilities, and resources devoted to biotechnology, and the objectives underlying those activities. The assessment shall include—

(1) a detailed analysis of efforts undertaken by the People's Republic of China (PRC) to acquire foreign-origin biotechnology, research and development, and genetic information, including technology owned by United States companies, research by United States institutions, and the genetic information of United States citizens;

(2) identification of PRC-based organizations conducting or directing these efforts, including information about the ties between those organizations and the PRC government, the Chinese Communist Party, or the People's Liberation Army; and

(3) a detailed analysis of the intelligence community resources devoted to biotechnology, including synthetic biology and genomic-related issues, and a plan to improve understanding of these issues and

ensure the intelligence community has the requisite expertise.

(c) FORM.—The assessment required under subsection (b) shall be submitted in unclassified form, but may include a classified annex, if necessary.

SEC. 354. UPDATES TO ANNUAL REPORTS ON INFLUENCE OPERATIONS AND CAMPAIGNS IN THE UNITED STATES BY THE CHINESE COMMUNIST PARTY.

Section 1107(b) of the National Security Act of 1947 (50 U.S.C. 3237(b)) is amended—

(1) by redesignating paragraph (9) as paragraph (10); and

(2) by inserting after paragraph (8) the following:

''(9) A listing of all known Chinese talent recruitment programs operating in the United States as of the date of the report.''.

SEC. 355. REPORT ON INFLUENCE OF PEOPLE'S REPUBLIC OF CHINA THROUGH BELT AND ROAD INITIATIVE PROJECTS WITH OTHER COUNTRIES.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on recent projects nego-

tiated by the People's Republic of China with other countries as part of the Belt and Road Initiative of the People's Republic of China. Such report shall include information about the types of such projects, costs of such projects, and the potential national security implications of such projects.

(b) FORM.—The report submitted under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 356. STUDY ON THE CREATION OF AN OFFICIAL DIGITAL CURRENCY BY THE PEOPLE'S REPUBLIC OF CHINA.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and

(3) the Committee on Financial Services, the Committee on Foreign Affairs, and the Committee on Appropriations of the House of Representatives.

(b) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the President shall sub-

mit to the appropriate committees of Congress a report on the short-, medium-, and long-term national security risks associated with the creation and use of the official digital renminbi of the People's Republic of China, including—

(1) risks arising from potential surveillance of transactions;

(2) risks related to security and illicit finance; and

(3) risks related to economic coercion and social control by the People's Republic of China.

(c) FORM OF REPORT.—The report required by subsection (b) shall be submitted in unclassified form, but may include a classified annex.

SEC. 357. REPORT ON EFFORTS OF CHINESE COMMUNIST PARTY TO ERODE FREEDOM AND AUTONOMY IN HONG KONG.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on efforts of the Chinese Communist Party to stifle political freedoms in Hong Kong, influence or manipulate the judiciary of Hong Kong, destroy freedom of the press and speech in Hong

Kong, and take actions to otherwise undermine the democratic processes of Hong Kong.

(b) CONTENTS.—The report submitted under subsection (a) shall include an assessment of the implications of the efforts of the Chinese Communist Party described in such subsection for international business, investors, academic institutions, and other individuals operating in Hong Kong.

(c) FORM.—The report submitted under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 358. REPORT ON TARGETING OF RENEWABLE SECTORS BY CHINA.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report assessing the efforts and advancements of China in the wind power, solar power, and electric vehicle battery production sectors (or key components of such sectors).

(b) CONTENTS.—The report submitted under subsection (a) shall include the following:

(1) An assessment of how China is targeting rare earth minerals and the effect of such targeting on the sectors described in subsection (a).

(2) Details of the use by the Chinese Communist Party of state-sanctioned forced labor schemes, including forced labor and the transfer of Uyghurs and other ethnic groups, and other human rights abuses in such sectors.

(c) FORM.—The report submitted under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

TITLE IV—ANOMALOUS HEALTH INCIDENTS

SEC. 401. DEFINITION OF ANOMALOUS HEALTH INCIDENT.

In this title, the term ''anomalous health incident'' means an unexplained health event characterized by any of a collection of symptoms and clinical signs that includes the sudden onset of perceived loud sound, a sensation of intense pressure or vibration in the head, possibly with a directional character, followed by the onset of tinnitus, hearing loss, acute disequilibrium, unsteady gait, visual disturbances, and ensuing cognitive dysfunction.

SEC. 402. ASSESSMENT AND REPORT ON INTERAGENCY COMMUNICATION RELATING TO EFFORTS TO ADDRESS ANOMALOUS HEALTH INCIDENTS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall—

(1) conduct an assessment of how the various elements of the intelligence community are coordinating or collaborating with each other and with elements of the Federal Government that are not part of the intelligence community in their efforts to address anomalous health incidents; and

(2) submit to the congressional intelligence committees a report on the findings of the Director with respect to the assessment conducted under paragraph (1).

(b) FORM.—The report submitted pursuant to subsection (a)(2) shall be submitted in unclassified form, but may include a classified annex.

SEC. 403. ADVISORY PANEL ON THE OFFICE OF MEDICAL SERVICES OF THE CENTRAL INTELLIGENCE AGENCY.

(a) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall establish, under the sponsorship of the National Institutes of Health and such other entities as the Director considers appropriate, an advisory panel to assess the capabilities, expertise, and qualifications of the Office of Medical Services of the Central Intelligence Agency in relation to the care and health management of personnel of the intelligence community who are

reporting symptoms consistent with anomalous health incidents.

(b) MEMBERSHIP.—

(1) IN GENERAL.—The advisory panel shall be composed of at least 9 individuals selected by the Director of National Intelligence from among individuals who are recognized experts in the medical profession and intelligence community.

(2) DIVERSITY.—In making appointments to the advisory panel, the Director shall ensure that the members of the panel reflect diverse experiences in the public and private sectors.

(c) DUTIES.—The duties of the advisory panel established under subsection (a) are as follows:

(1) To review the performance of the Office of Medical Services of the Central Intelligence Agency, specifically as it relates to the medical care of personnel of the intelligence community who are reporting symptoms consistent with anomalous health incidents during the period beginning on January 1, 2016, and ending on December 31, 2021.

(2) To assess the policies and procedures that guided external treatment referral practices for Office of Medical Services patients who reported symp-

toms consistent with anomalous health incidents during the period described in paragraph (1).

(3) To develop recommendations regarding capabilities, processes, and policies to improve patient treatment by the Office of Medical Services with regard to anomalous health incidents, including with respect to access to external treatment facilities and specialized medical care.

(4) To prepare and submit a report as required by subsection (e)(1).

(d) ADMINISTRATIVE MATTERS.—

(1) IN GENERAL.—The Director of the Central Intelligence Agency shall provide the advisory panel established pursuant to subsection (a) with timely access to appropriate information, data, resources, and analysis so that the advisory panel may carry out the duties of the advisory panel under subsection (c).

(2) INAPPLICABILITY OF FACA.—The requirements of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the advisory panel established pursuant to subsection (a).

(e) REPORTS.—

(1) FINAL REPORT.—Not later than 1 year after the date on which the Director of National In-

telligence establishes the advisory panel pursuant to subsection (a), the advisory panel shall submit to the Director of National Intelligence, the Director of the Central Intelligence Agency, and the congressional intelligence committees a final report on the activities of the advisory panel under this section.

(2) ELEMENTS.—The final report submitted under paragraph (1) shall contain a detailed statement of the findings and conclusions of the panel, including—

(A) a history of anomalous health incidents; and

(B) such additional recommendations for legislation or administrative action as the advisory panel considers appropriate.

(3) INTERIM REPORT OR BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report or provide such committees a briefing on the interim findings of the advisory panel with respect to the elements set forth in paragraph (2).

(4) COMMENTS OF THE DIRECTOR OF NATIONAL INTELLIGENCE.—Not later than 30 days after receiving the final report of the advisory panel

under paragraph (1), the Director of National Intelligence shall submit to the congressional intelligence committees such comments as the Director may have with respect to such report.

SEC. 404. JOINT TASK FORCE TO INVESTIGATE ANOMALOUS HEALTH INCIDENTS.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

(b) JOINT TASK FORCE REQUIRED.—The Director of National Intelligence and the Director of the Federal Bureau of Investigation shall jointly establish a task force to investigate anomalous health incidents.

(c) CONSULTATION.—In carrying out an investigation under subsection (b), the task force established under such subsection shall consult with the Secretary of Defense.

(d) REPORT TO CONGRESS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the task force established under subsection (b) shall complete the investigation required by such subsection and submit to the appropriate committees of Congress a written report on the findings of the task force with respect to such investigation.

(2) FORM.—The report submitted pursuant to paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

SEC. 405. REPORTING ON OCCURRENCE OF ANOMALOUS HEALTH INCIDENTS.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Appropriations of the Senate; and

(3) the Committee on Appropriations of the House of Representatives.

(b) IN GENERAL.—Whenever the head of an element of the intelligence community becomes aware of a report of an anomalous health incident occurring among the employees or contractors of the element, the head of the ele-

ment shall submit to the appropriate committees of Congress a brief report on the reported incident.

SEC. 406. ACCESS TO CERTAIN FACILITIES OF UNITED STATES GOVERNMENT FOR ASSESSMENT OF ANOMALOUS HEALTH CONDITIONS.

(a) ASSESSMENT.—The Director of National Intelligence shall ensure that elements of the intelligence community provide to employees of elements of the intelligence community and their family members who are experiencing symptoms of anomalous health conditions timely access for medical assessment to facilities of the United States Government with expertise in traumatic brain injury.

(b) PROCESS FOR ASSESSMENT AND TREATMENT.—The Director of National Intelligence shall coordinate with the Secretary of Defense and the heads of such Federal agencies as the Director considers appropriate to ensure there is a process to provide employees and their family members described in subsection (a) with timely access to the National Intrepid Center of Excellence at Walter Reed National Military Medical Center for assessment and, if necessary, treatment, by not later than 60 days after the date of the enactment of this Act.

TITLE V—SECURITY CLEARANCES AND TRUSTED WORKFORCE

SEC. 501. EXCLUSIVITY, CONSISTENCY, AND TRANSPARENCY IN SECURITY CLEARANCE PROCEDURES, AND RIGHT TO APPEAL.

(a) EXCLUSIVITY OF PROCEDURES.—Section 801 of the National Security Act of 1947 (50 U.S.C. 3161) is amended by adding at the end the following:

''(c) EXCLUSIVITY.—Except as provided in subsection (b) and subject to sections 801A and 801B, the procedures established pursuant to subsection (a) and promulgated and set forth under part 2001 of title 32, Code of Federal Regulations, or successor regulations, shall be the exclusive procedures by which decisions about eligibility for access to classified information are governed.''.

(b) TRANSPARENCY.—Such section is further amended by adding at the end the following:

''(d) PUBLICATION.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection, the President shall—

''(A) publish in the Federal Register the procedures established pursuant to subsection (a); or

"(B) submit to Congress a certification that the procedures currently in effect that govern access to classified information as described in subsection (a)—

"(i) are published in the Federal Register; and

"(ii) comply with the requirements of subsection (a).

"(2) UPDATES.—Whenever the President makes a revision to a procedure established pursuant to subsection (a), the President shall publish such revision in the Federal Register not later than 30 days before the date on which the revision becomes effective.".

(c) CONSISTENCY.—

(1) IN GENERAL.—Title VIII of the National Security Act of 1947 (50 U.S.C. 3161 et seq.) is amended by inserting after section 801 the following:

"SEC. 801A. DECISIONS RELATING TO ACCESS TO CLASSIFIED INFORMATION.

"(a) DEFINITIONS.—In this section:

"(1) AGENCY.—The term 'agency' has the meaning given the term 'Executive agency' in section 105 of title 5, United States Code.

''(2) CLASSIFIED INFORMATION.—The term 'classified information' includes sensitive compartmented information, restricted data, restricted handling information, and other compartmented information.

''(3) ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION.—The term 'eligibility for access to classified information' has the meaning given such term in the procedures established pursuant to section 801(a).

''(b) IN GENERAL.—Each head of an agency that makes a determination regarding eligibility for access to classified information shall ensure that in making the determination, the head of the agency or any person acting on behalf of the head of the agency—

''(1) does not violate any right or protection enshrined in the Constitution of the United States, including rights articulated in the First, Fifth, and Fourteenth Amendments;

''(2) does not discriminate for or against an individual on the basis of race, ethnicity, color, religion, sex, national origin, age, or handicap;

''(3) is not carrying out—

''(A) retaliation for political activities or beliefs; or

''(B) a coercion or reprisal described in section 2302(b)(3) of title 5, United States Code; and

''(4) does not violate section 3001(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)).''.

(2) CLERICAL AMENDMENT.—The table of contents in the matter preceding section 2 of the National Security Act of 1947 (50 U.S.C. 3002) is amended by inserting after the item relating to section 801 the following:

''Sec. 801A. Decisions relating to access to classified information.''.

(d) RIGHT TO APPEAL.—

(1) IN GENERAL.—Such title, as amended by subsection (c), is further amended by inserting after section 801A the following:

''SEC. 801B. RIGHT TO APPEAL.

''(a) DEFINITIONS.—In this section:

''(1) AGENCY.—The term 'agency' has the meaning given the term 'Executive agency' in section 105 of title 5, United States Code.

''(2) COVERED PERSON.—The term 'covered person' means a person, other than the President and Vice President, currently or formerly employed in, detailed to, assigned to, or issued an authorized conditional offer of employment for a position that

requires access to classified information by an agency, including the following:

"(A) A member of the Armed Forces.

"(B) A civilian.

"(C) An expert or consultant with a contractual or personnel obligation to an agency.

"(D) Any other category of person who acts for or on behalf of an agency as determined by the head of the agency.

"(3) ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION.—The term 'eligibility for access to classified information' has the meaning given such term in the procedures established pursuant to section 801(a).

"(4) NEED FOR ACCESS.—The term 'need for access' has such meaning as the President may define in the procedures established pursuant to section 801(a).

"(5) RECIPROCITY OF CLEARANCE.—The term 'reciprocity of clearance', with respect to a denial by an agency, means that the agency, with respect to a covered person—

"(A) failed to accept a security clearance background investigation as required by paragraph (1) of section 3001(d) of the Intelligence

Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(d));

"(B) failed to accept a transferred security clearance background investigation required by paragraph (2) of such section;

"(C) subjected the covered person to an additional investigative or adjudicative requirement in violation of paragraph (3) of such section; or

"(D) conducted an investigation in violation of paragraph (4) of such section.

"(6) SECURITY EXECUTIVE AGENT.—The term 'Security Executive Agent' means the officer serving as the Security Executive Agent pursuant to section 803.

"(b) AGENCY REVIEW.—

"(1) IN GENERAL.—Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, each head of an agency shall, consistent with the interests of national security, establish and publish in the Federal Register a process by which a covered person to whom eligibility for access to classified information was denied or revoked by the agency or for whom reciprocity of clearance was denied by the agency

can appeal that denial or revocation within the agency.

''(2) ELEMENTS.—The process required by paragraph (1) shall include the following:

''(A) In the case of a covered person to whom eligibility for access to classified information or reciprocity of clearance is denied or revoked by an agency, the following:

''(i) The head of the agency shall provide the covered person with a written—

''(I) detailed explanation of the basis for the denial or revocation as the head of the agency determines is consistent with the interests of national security and as permitted by other applicable provisions of law; and

''(II) notice of the right of the covered person to a hearing and appeal under this subsection.

''(ii) Not later than 30 days after receiving a request from the covered person for copies of the documents that formed the basis of the agency's decision to revoke or deny, including the investigative file, the

head of the agency shall provide to the covered person copies of such documents as—

"(I) the head of the agency determines is consistent with the interests of national security; and

"(II) permitted by other applicable provisions of law, including—

"(aa) section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act');

"(bb) section 552a of such title (commonly known as the 'Privacy Act of 1974'); and

"(cc) such other provisions of law relating to the protection of confidential sources and privacy of individuals.

"(iii)(I) The covered person shall have the opportunity to retain counsel or other representation at the covered person's expense.

"(II) Upon the request of the covered person, and a showing that the ability to review classified information is essential to

the resolution of an appeal under this subsection, counsel or other representation retained under this clause shall be considered for access to classified information for the limited purposes of such appeal.

''(iv)(I) The head of the agency shall provide the covered person an opportunity, at a point in the process determined by the agency head—

''(aa) to appear personally before an adjudicative or other authority, other than the investigating entity, and to present to such authority relevant documents, materials, and information, including evidence that past problems relating to the denial or revocation have been overcome or sufficiently mitigated; and

''(bb) to call and cross-examine witnesses before such authority, unless the head of the agency determines that calling and cross-examining witnesses is not consistent with the interests of national security.

"(II) The head of the agency shall make, as part of the security record of the covered person, a written summary, transcript, or recording of any appearance under item (aa) of subclause (I) or of any calling or cross-examining of witnesses under item (bb) of such subclause.

"(v) On or before the date that is 30 days after the date on which the covered person receives copies of documents under clause (ii), the covered person may request a hearing of the decision to deny or revoke by filing a written appeal with the head of the agency.

"(B) A requirement that each review of a decision under this subsection is completed on average not later than 180 days after the date on which a hearing is requested under subparagraph (A)(v).

"(3) AGENCY REVIEW PANELS.—

"(A) IN GENERAL.—Each head of an agency shall establish a panel to hear and review appeals under this subsection.

"(B) MEMBERSHIP.—

"(i) COMPOSITION.—Each panel established by the head of an agency under subparagraph (A) shall be composed of at least 3 employees of the agency selected by the agency head, two of whom shall not be members of the security field.

"(ii) TERMS.—A term of service on a panel established by the head of an agency under subparagraph (A) shall not exceed 2 years.

"(C) DECISIONS.—

"(i) WRITTEN.—Each decision of a panel established under subparagraph (A) shall be in writing and contain a justification of the decision.

"(ii) CONSISTENCY.—Each head of an agency that establishes a panel under subparagraph (A) shall ensure that each decision of the panel is consistent with the interests of national security and applicable provisions of law.

"(iii) OVERTURN.—The head of an agency may overturn a decision of the panel if, not later than 30 days after the date on which the panel issues the deci-

sion, the agency head personally exercises the authority granted by this clause to overturn such decision.

"(iv) FINALITY.—Each decision of a panel established under subparagraph (A) or overturned pursuant to clause (iii) of this subparagraph shall be final but subject to appeal and review under subsection (c).

"(D) ACCESS TO CLASSIFIED INFORMATION.—The head of an agency that establishes a panel under subparagraph (A) shall afford access to classified information to the members of the panel as the agency head determines—

"(i) necessary for the panel to hear and review an appeal under this subsection; and

"(ii) consistent with the interests of national security.

"(4) REPRESENTATION BY COUNSEL.—

"(A) IN GENERAL.—Each head of an agency shall ensure that, under this subsection, a covered person appealing a decision of the head's agency under this subsection has an op-

portunity to retain counsel or other representation at the covered person's expense.

"(B) ACCESS TO CLASSIFIED INFORMATION.—

"(i) IN GENERAL.—Upon the request of a covered person appealing a decision of an agency under this subsection and a showing that the ability to review classified information is essential to the resolution of the appeal under this subsection, the head of the agency shall sponsor an application by the counsel or other representation retained under this paragraph for access to classified information for the limited purposes of such appeal.

"(ii) EXTENT OF ACCESS.—Counsel or another representative who is cleared for access under this subparagraph may be afforded access to relevant classified materials to the extent consistent with the interests of national security.

"(5) CORRECTIVE ACTION.—If, in the course of proceedings under this subsection, the head of an agency or a panel established by the agency head under paragraph (3) decides that a covered person's

eligibility for access to classified information was improperly denied or revoked by the agency, the agency shall take corrective action to return the covered person, as nearly as practicable and reasonable, to the position such covered person would have held had the improper denial or revocation not occurred.

"(6) PUBLICATION OF DECISIONS.—

"(A) IN GENERAL.—Each head of an agency shall publish each final decision on an appeal under this subsection.

"(B) REQUIREMENTS.—In order to ensure transparency, oversight by Congress, and meaningful information for those who need to understand how the clearance process works, each publication under subparagraph (A) shall be—

"(i) made in a manner that is consistent with section 552 of title 5, United States Code, as amended by the Electronic Freedom of Information Act Amendments of 1996 (Public Law 104–231);

"(ii) published to explain the facts of the case, redacting personally identifiable information and sensitive program information; and

"(iii) made available on a website that is searchable by members of the public.

"(c) HIGHER LEVEL REVIEW.—

"(1) PANEL.—

"(A) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, the Security Executive Agent shall establish a panel to review decisions made on appeals pursuant to the processes established under subsection (b).

"(B) SCOPE OF REVIEW AND JURISDICTION.—After the initial review to verify grounds for appeal, the panel established under subparagraph (A) shall review such decisions only—

"(i) as they relate to violations of section 801A(b); or

"(ii) to the extent to which an agency properly conducted a review of an appeal under subsection (b).

"(C) COMPOSITION.—The panel established pursuant to subparagraph (A) shall be composed of three individuals selected by the Security Executive Agent for purposes of the

panel, of whom at least one shall be an attorney.

"(2) APPEALS AND TIMELINESS.—

"(A) APPEALS.—

"(i) INITIATION.—On or before the date that is 30 days after the date on which a covered person receives a written decision on an appeal under subsection (b), the covered person may initiate oversight of that decision by filing a written appeal with the Security Executive Agent.

"(ii) FILING.—A written appeal filed under clause (i) relating to a decision of an agency shall be filed in such form, in such manner, and containing such information as the Security Executive Agent may require, including—

"(I) a description of—

"(aa) any alleged violations of section 801A(b) relating to the denial or revocation of the covered person's eligibility for access to classified information; and

"(bb) any allegations of how the decision may have been the

result of the agency failing to properly conduct a review under subsection (b); and

"(II) supporting materials and information for the allegations described under subclause (I).

"(B) TIMELINESS.—The Security Executive Agent shall ensure that, on average, review of each appeal filed under this subsection is completed not later than 180 days after the date on which the appeal is filed.

"(3) DECISIONS AND REMANDS.—

"(A) IN GENERAL.—If, in the course of reviewing under this subsection a decision of an agency under subsection (b), the panel established under paragraph (1) decides that there is sufficient evidence of a violation of section 801A(b) to merit a new hearing or decides that the decision of the agency was the result of an improperly conducted review under subsection (b), the panel shall vacate the decision made under subsection (b) and remand to the agency by which the covered person shall be eligible for a new appeal under subsection (b).

"(B) WRITTEN DECISIONS.—Each decision of the panel established under paragraph (1) shall be in writing and contain a justification of the decision.

"(C) CONSISTENCY.—The panel under paragraph (1) shall ensure that each decision of the panel is consistent with the interests of national security and applicable provisions of law.

"(D) FINALITY.—

"(i) IN GENERAL.—Except as provided in clause (ii), each decision of the panel established under paragraph (1) shall be final.

"(ii) OVERTURN.—The Security Executive Agent may overturn a decision of the panel if, not later than 30 days after the date on which the panel issues the decision, the Security Executive Agent personally exercises the authority granted by this clause to overturn such decision.

"(E) NATURE OF REMANDS.—In remanding a decision under subparagraph (A), the panel established under paragraph (1) may not direct the outcome of any further appeal under subsection (b).

''(F) NOTICE OF DECISIONS.—For each decision of the panel established under paragraph (1) regarding a covered person, the Security Executive Agent shall provide the covered person with a written notice of the decision that includes a detailed description of the reasons for the decision, consistent with the interests of national security and applicable provisions of law.

''(4) REPRESENTATION BY COUNSEL.—

''(A) IN GENERAL.—The Security Executive Agent shall ensure that, under this subsection, a covered person appealing a decision under subsection (b) has an opportunity to retain counsel or other representation at the covered person's expense.

''(B) ACCESS TO CLASSIFIED INFORMATION.—

''(i) IN GENERAL.—Upon the request of the covered person and a showing that the ability to review classified information is essential to the resolution of an appeal under this subsection, the Security Executive Agent shall sponsor an application by the counsel or other representation re-

tained under this paragraph for access to classified information for the limited purposes of such appeal.

"(ii) EXTENT OF ACCESS.—Counsel or another representative who is cleared for access under this subparagraph may be afforded access to relevant classified materials to the extent consistent with the interests of national security.

"(5) ACCESS TO DOCUMENTS AND EMPLOYEES.—

"(A) AFFORDING ACCESS TO MEMBERS OF PANEL.—The Security Executive Agent shall afford access to classified information to the members of the panel established under paragraph (1)(A) as the Security Executive Agent determines—

"(i) necessary for the panel to review a decision described in such paragraph; and

"(ii) consistent with the interests of national security.

"(B) AGENCY COMPLIANCE WITH REQUESTS OF PANEL.—Each head of an agency shall comply with each request by the panel for

a document and each request by the panel for access to employees of the agency necessary for the review of an appeal under this subsection, to the degree that doing so is, as determined by the head of the agency and permitted by applicable provisions of law, consistent with the interests of national security.

''(6) PUBLICATION OF DECISIONS.—

''(A) IN GENERAL.—For each final decision on an appeal under this subsection, the head of the agency with respect to which the appeal pertains and the Security Executive Agent shall each publish the decision, consistent with the interests of national security.

''(B) REQUIREMENTS.—In order to ensure transparency, oversight by Congress, and meaningful information for those who need to understand how the clearance process works, each publication under subparagraph (A) shall be—

''(i) made in a manner that is consistent with section 552 of title 5, United States Code, as amended by the Electronic Freedom of Information Act Amendments of 1996 (Public Law 104–231);

"(ii) published to explain the facts of the case, redacting personally identifiable information and sensitive program information; and

"(iii) made available on a website that is searchable by members of the public.

"(d) PERIOD OF TIME FOR THE RIGHT TO APPEAL.—

"(1) IN GENERAL.—Except as provided in paragraph (2), any covered person who has been the subject of a decision made by the head of an agency to deny or revoke eligibility for access to classified information shall retain all rights to appeal under this section until the conclusion of the appeals process under this section.

"(2) WAIVER OF RIGHTS.—

"(A) PERSONS.—Any covered person may voluntarily waive the covered person's right to appeal under this section and such waiver shall be conclusive.

"(B) AGENCIES.—The head of an agency may not require a covered person to waive the covered person's right to appeal under this section for any reason.

''(e) WAIVER OF AVAILABILITY OF PROCEDURES FOR NATIONAL SECURITY INTEREST.—

''(1) IN GENERAL.—If the head of an agency determines that a procedure established under subsection (b) cannot be made available to a covered person in an exceptional case without damaging a national security interest of the United States by revealing classified information, such procedure shall not be made available to such covered person.

''(2) FINALITY.—A determination under paragraph (1) shall be final and conclusive and may not be reviewed by any other official or by any court.

''(3) REPORTING.—

''(A) CASE-BY-CASE.—

''(i) IN GENERAL.—In each case in which the head of an agency determines under paragraph (1) that a procedure established under subsection (b) cannot be made available to a covered person, the agency head shall, not later than 30 days after the date on which the agency head makes such determination, submit to the Security Executive Agent and to the congressional intelligence committees a report stating the reasons for the determination.

"(ii) FORM.—A report submitted under clause (i) may be submitted in classified form as necessary.

"(B) ANNUAL REPORTS.—

"(i) IN GENERAL.—Not less frequently than once each fiscal year, the Security Executive Agent shall submit to the congressional intelligence committees a report on the determinations made under paragraph (1) during the previous fiscal year.

"(ii) CONTENTS.—Each report submitted under clause (i) shall include, for the period covered by the report, the following:

"(I) The number of cases and reasons for determinations made under paragraph (1), disaggregated by agency.

"(II) Such other matters as the Security Executive Agent considers appropriate.

"(f) DENIALS AND REVOCATIONS UNDER OTHER PROVISIONS OF LAW.—

''(1) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit or affect the responsibility and power of the head of an agency to deny or revoke eligibility for access to classified information or to deny reciprocity of clearance in the interest of national security.

''(2) DENIALS AND REVOCATION.—The power and responsibility to deny or revoke eligibility for access to classified information or to deny reciprocity of clearance pursuant to any other provision of law or Executive order may be exercised only when the head of an agency determines that an applicable process established under this section cannot be invoked in a manner that is consistent with national security.

''(3) FINALITY.—A determination under paragraph (2) shall be final and conclusive and may not be reviewed by any other official or by any court.

''(4) REPORTING.—

''(A) CASE-BY-CASE.—

''(i) IN GENERAL.—In each case in which the head of an agency determines under paragraph (2) that a determination relating to a denial or revocation of eligibility for access to classified information or

denial of reciprocity of clearance could not be made pursuant to a process established under this section, the agency head shall, not later than 30 days after the date on which the agency head makes such a determination under paragraph (2), submit to the Security Executive Agent and to the congressional intelligence committees a report stating the reasons for the determination.

''(ii) FORM.—A report submitted under clause (i) may be submitted in classified form as necessary.

''(B) ANNUAL REPORTS.—

''(i) IN GENERAL.—Not less frequently than once each fiscal year, the Security Executive Agent shall submit to the congressional intelligence committees a report on the determinations made under paragraph (2) during the previous fiscal year.

''(ii) CONTENTS.—Each report submitted under clause (i) shall include, for the period covered by the report, the following:

"(I) The number of cases and reasons for determinations made under paragraph (2), disaggregated by agency.

"(II) Such other matters as the Security Executive Agent considers appropriate.

"(g) RELATIONSHIP TO SUITABILITY.—No person may use a determination of suitability under part 731 of title 5, Code of Federal Regulations, or successor regulation, for the purpose of denying a covered person the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information or a denial of reciprocity of clearance.

"(h) PRESERVATION OF ROLES AND RESPONSIBILITIES UNDER EXECUTIVE ORDER 10865 AND OF THE DEFENSE OFFICE OF HEARINGS AND APPEALS.—Nothing in this section shall be construed to diminish or otherwise affect the procedures in effect on the day before the date of the enactment of this Act for denial and revocation procedures provided to individuals by Executive Order 10865 (50 U.S.C. 3161 note; relating to safeguarding classified information within industry), or successor order, including those administered through the Defense Office of Hearings and Appeals of the Department of Defense under De-

partment of Defense Directive 5220.6, or successor directive.

''(i) RULE OF CONSTRUCTION RELATING TO CERTAIN OTHER PROVISIONS OF LAW.—This section and the processes and procedures established under this section shall not be construed to apply to paragraphs (6) and (7) of section 3001(j) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)).''.

(2) CLERICAL AMENDMENT.—The table of contents in the matter preceding section 2 of the National Security Act of 1947 (50 U.S.C. 3002), as amended by subsection (c), is further amended by inserting after the item relating to section 801A the following:

''Sec. 801B. Right to appeal.''.

SEC. 502. FEDERAL POLICY ON SHARING OF DEROGATORY INFORMATION PERTAINING TO CONTRACTOR EMPLOYEES IN THE TRUSTED WORKFORCE.

(a) POLICY REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Security Executive Agent, in coordination with the principal members of the Performance Accountability Council and the Attorney General, shall issue a policy for the Federal Government on sharing of derogatory information pertaining to contractor employees engaged by the Federal Government.

(b) CONSENT REQUIREMENT.—

(1) IN GENERAL.—The policy issued under subsection (a) shall require, as a condition of accepting a security clearance with the Federal Government, that a contractor employee provide prior written consent for the Federal Government to share covered derogatory information with the chief security officer of the contractor employer that employs the contractor employee.

(2) COVERED DEROGATORY INFORMATION.—For purposes of this section, covered derogatory information—

(A) is information that—

(i) contravenes National Security Adjudicative Guidelines as specified in Security Executive Agent Directive 4 (appendix A to part 710 of title 10, Code of Federal Regulations), or any successor Federal policy;

(ii) a Federal Government agency certifies is accurate and reliable;

(iii) is relevant to a contractor's ability to protect against insider threats as required by section 1–202 of the National Industrial Security Program Operating

Manual (NISPOM), or successor manual; and

(iv) may have a bearing on the contractor employee's suitability for a position of public trust or to receive credentials to access certain facilities of the Federal Government; and

(B) shall include any negative information considered in the adjudicative process, including information provided by the contractor employee on forms submitted for the processing of the contractor employee's security clearance.

(c) ELEMENTS.—The policy issued under subsection (a) shall—

(1) require Federal agencies, except under exceptional circumstances specified by the Security Executive Agent, to share with the contractor employer of a contractor employee engaged with the Federal Government the existence of potentially derogatory information and which National Security Adjudicative Guideline it falls under, with the exception that the Security Executive Agent may waive such requirement in circumstances the Security Executive Agent considers extraordinary;

(2) require that covered derogatory information shared with a contractor employer as described in subsection (b)(1) be used by the contractor employer exclusively for risk mitigation purposes under section 1–202 of the National Industrial Security Program Operating Manual, or successor manual;

(3) require Federal agencies to share any mitigation measures in place to address the derogatory information;

(4) establish standards for timeliness for sharing the derogatory information;

(5) specify the methods by which covered derogatory information will be shared with the contractor employer of the contractor employee;

(6) allow the contractor employee, within a specified timeframe, the right—

(A) to contest the accuracy and reliability of covered derogatory information;

(B) to address or remedy any concerns raised by the covered derogatory information; and

(C) to provide documentation pertinent to subparagraph (A) or (B) for an agency to place in relevant security clearance databases;

(7) establish a procedure by which the contractor employer of the contractor employee may consult with the Federal Government prior to taking any remedial action under section 1–202 of the National Industrial Security Program Operating Manual, or successor manual, to address the derogatory information the Federal agency has provided;

(8) stipulate that the chief security officer of the contractor employer is prohibited from sharing or discussing covered derogatory information with other parties, including nonsecurity professionals at the contractor employer; and

(9) require companies in the National Industrial Security Program to comply with the policy.

(d) CONSIDERATION OF LESSONS LEARNED FROM INFORMATION-SHARING PROGRAM FOR POSITIONS OF TRUST AND SECURITY CLEARANCES.—In developing the policy issued under subsection (a), the Director shall consider, to the extent available, lessons learned from actions taken to carry out section 6611(f) of the National Defense Authorization Act for Fiscal Year 2020 (50 U.S.C. 3352f(f)).

SEC. 503. PERFORMANCE MEASURES REGARDING TIMELINESS FOR PERSONNEL MOBILITY.

(a) POLICY REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall issue a policy for measuring the total time it takes to transfer personnel with security clearances and eligibility for access to information commonly referred to as ''sensitive compartmented information'' (SCI) from one Federal agency to another, or from one contract to another in the case of a contractor.

(b) REQUIREMENTS.—The policy issued under subsection (a) shall—

(1) to the degree practicable, cover all personnel who are moving to positions that require a security clearance and access to sensitive compartmented information;

(2) cover the period from the first time a Federal agency or company submits a request to a Federal agency for the transfer of the employment of an individual with a clearance access or eligibility determination to another Federal agency, to the time the individual is authorized by that receiving agency to start to work in the new position; and

(3) include analysis of all appropriate phases of the process, including polygraph, suitability determination, fitness determination, human resources re-

view, transfer of the sensitive compartmented information access, and contract actions.

(c) UPDATED POLICIES.—

(1) MODIFICATIONS.—Not later than 1 year after the date on which the Director issues the policy under subsection (a), the Director shall issue modifications to such policies as the Director determines were issued before the issuance of the policy under such subsection and are relevant to such updated policy, as the Director considers appropriate.

(2) RECOMMENDATIONS.—Not later than 1 year after the date on which the Director issues the policy under subsection (a), the Director shall submit to Congress recommendations for legislative action to update metrics specified elsewhere in statute to measure parts of the process that support transfers described in subsection (a).

(d) ANNUAL REPORTS.—Not later than 180 days after issuing the policy required by subsection (a) and not less frequently than once each year thereafter until the date that is 3 years after the date of such issuance, the Director shall submit to Congress a report on the implementation of such policy. Such report shall address performance by agency and by clearance type in meeting such policy.

SEC. 504. GOVERNANCE OF TRUSTED WORKFORCE 2.0 INITIATIVE.

(a) GOVERNANCE.—The Director of National Intelligence, acting as the Security Executive Agent, and the Director of the Office of Personnel Management, acting as the Suitability and Credentialing Executive Agent, in coordination with the Deputy Director for Management in the Office of Management and Budget, acting as the director of the Performance Accountability Council, and the Under Secretary of Defense for Intelligence and Security shall jointly—

(1) not later than 180 days after the date of the enactment of this Act, publish in the Federal Register a policy with guidelines and standards for Federal Government agencies and industry partners to implement the Trusted Workforce 2.0 initiative;

(2) not later than 2 years after the date of the enactment of this Act and not less frequently than once every 6 months thereafter, submit to Congress a report on the timing, delivery, and adoption of Federal Government agencies' policies, products, and services to implement the Trusted Workforce 2.0 initiative, including those associated with the National Background Investigation Service; and

(3) not later than 90 days after the date of the enactment of this Act, submit to Congress perform-

ance management metrics for the implementation of the Trusted Workforce 2.0 initiative, including performance metrics regarding timeliness, cost, and measures of effectiveness.

(b) INDEPENDENT STUDY ON TRUSTED WORKFORCE 2.0.—

(1) STUDY REQUIRED.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence shall enter into an agreement with an entity that is not part of the Federal Government to conduct a study on the effectiveness of the initiatives of the Federal Government known as Trusted Workforce 1.25, 1.5, and 2.0.

(2) ELEMENTS.—The study required by paragraph (1) shall include the following:

(A) An assessment of how effective such initiatives are or will be in determining who should or should not have access to classified information.

(B) A comparison of the effectiveness of such initiatives with the system of periodic reinvestigations that was in effect on the day before the date of the enactment of this Act.

(C) Identification of what is lost from the suspension of universal periodic reinvestigations in favor of a system of continuous vetting.

(D) An assessment of the relative effectiveness of Trusted Workforce 1.25, Trusted Workforce 1.5, and Trusted Workforce 2.0.

(3) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director shall submit a report on the findings from the study conducted under paragraph (1) to the following:

(A) The congressional intelligence committees.

(B) The Committee on Armed Services of the Senate.

(C) The Committee on Homeland Security and Governmental Affairs of the Senate.

(D) The Committee on Armed Services of the House of Representatives.

(E) The Committee on Homeland Security of the House of Representatives.

TITLE VI—OTHER INTELLIGENCE MATTERS

SEC. 601. NATIONAL TECHNOLOGY STRATEGY.

(a) IN GENERAL.—Each year, the President shall submit to Congress a comprehensive report on the tech-

nology strategy of the United States designed to maintain United States leadership in critical and emerging technologies essential to United States national security and economic prosperity.

(b) ELEMENTS.—Each National Technology Strategy developed and submitted under subsection (a) shall contain at least the following elements:

(1) An assessment of the efforts of the United States Government to preserve United States leadership in key emerging technologies and prevent United States strategic competitors from leveraging advanced technologies to gain strategic military or economic advantages over the United States.

(2) A review of existing United States Government technology policy, including long-range goals.

(3) An analysis of technology trends and assessment of the relative competitiveness of United States technology sectors in relation to strategic competitors.

(4) Identification of sectors critical for the long-term resilience of United States innovation leadership across design, manufacturing, supply chains, and markets.

(5) Recommendations for domestic policy incentives to sustain an innovation economy and develop

specific, high-cost sectors necessary for long-term national security ends.

(6) Recommendations for policies to protect United States and leadership of allies of the United States in critical areas through targeted export controls, investment screening, and counterintelligence activities.

(7) Identification of priority domestic research and development areas critical to national security and necessary to sustain United States leadership, and directing funding to fill gaps in basic and applied research where the private sector does not focus.

(8) Recommendations for talent programs to grow United States talent in key critical and emerging technologies and enhance the ability of the Federal Government to recruit and retain individuals with critical skills into Federal service.

(9) Methods to foster the development of international partnerships to reinforce domestic policy actions, build new markets, engage in collaborative research, and create an international environment that reflects United States values and protects United States interests.

(10) A technology annex, which may be classified, to establish an integrated and enduring approach to the identification, prioritization, development, and fielding of emerging technologies.

(11) Such other information as may be necessary to help inform Congress on matters relating to the technology strategy of the United States and related implications for United States national security.

SEC. 602. IMPROVEMENTS RELATING TO CONTINUITY OF PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD MEMBERSHIP.

Paragraph (4) of section 1061(h) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(h)) is amended to read as follows:

''(4) TERM.—

''(A) COMMENCEMENT.—Each member of the Board shall serve a term of 6 years, commencing on the date of the appointment of the member to the Board.

''(B) REAPPOINTMENT.—A member may be reappointed to one or more additional terms.

''(C) VACANCY.—A vacancy in the Board shall be filled in the manner in which the original appointment was made.

''(D) EXTENSION.—Upon the expiration of the term of office of a member, the member may continue to serve, at the election of the member—

''(i) during the period preceding the reappointment of the member pursuant to subparagraph (B); or

''(ii) until the member's successor has been appointed and qualified.''.

SEC. 603. AIR AMERICA.

(a) FINDINGS.—Congress finds the following:

(1) Air America, Incorporated (referred to in this section as ''Air America'') and its related cover corporate entities were wholly owned and controlled by the United States Government and directed and managed by the Department of Defense, the Department of State, and the Central Intelligence Agency from 1950 to 1976.

(2) Air America, a corporation owned by the Government of the United States, constituted a ''Government corporation'', as defined in section 103 of title 5, United States Code.

(3) It is established that the employees of Air America and the other entities described in paragraph (1) were Federal employees.

(4) The employees of Air America were retroactively excluded from the definition of the term ''employee'' under section 2105 of title 5, United States Code, on the basis of an administrative policy change in paperwork requirements implemented by the Office of Personnel Management 10 years after the service of the employees had ended and, by extension, were retroactively excluded from the definition of the term ''employee'' under section 8331 of title 5, United States Code, for retirement credit purposes.

(5) The employees of Air America were paid as Federal employees, with salaries subject to—

(A) the General Schedule under subchapter III of chapter 53 of title 5, United States Code; and

(B) the rates of basic pay payable to members of the Armed Forces.

(6) The service and sacrifice of the employees of Air America included—

(A) suffering a high rate of casualties in the course of employment;

(B) saving thousands of lives in search and rescue missions for downed United States airmen and allied refugee evacuations; and

(C) lengthy periods of service in challenging circumstances abroad.

(b) DEFINITIONS.—In this section:

(1) AFFILIATED COMPANY.—The term ''affiliated company'', with respect to Air America, includes Air Asia Company Limited, CAT Incorporated, Civil Air Transport Company Limited, and the Pacific Division of Southern Air Transport.

(2) QUALIFYING SERVICE.—The term ''qualifying service'' means service that—

(A) was performed by a United States citizen as an employee of Air America or an affiliated company during the period beginning on January 1, 1950, and ending on December 31, 1976; and

(B) is documented in the attorney-certified corporate records of Air America or any affiliated company.

(c) TREATMENT AS FEDERAL EMPLOYMENT.—Any period of qualifying service—

(1) is deemed to have been service of an employee (as defined in section 2105 of title 5, United States Code) with the Federal Government; and

(2) shall be treated as creditable service by an employee for purposes of subchapter III of chapter 83 of title 5, United States Code.

(d) RIGHTS.—An individual who performed qualifying service, or a survivor of such an individual, shall be entitled to the rights, retroactive as applicable, provided to employees and their survivors for creditable service under the Civil Service Retirement System under subchapter III of chapter 83 of title 5, United States Code, with respect to that qualifying service.

(e) DEDUCTION, CONTRIBUTION, AND DEPOSIT REQUIREMENTS.—The deposit of funds in the Treasury of the United States made by Air America in the form of a lump-sum payment apportioned in part to the Civil Service Disability & Retirement Fund in 1976 is deemed to satisfy the deduction, contribution, and deposit requirements under section 8334 of title 5, United States Code, with respect to all periods of qualifying service.

(f) APPLICATION TIME LIMIT.—Section 8345(i)(2) of title 5, United States Code, shall be applied with respect to the death of an individual who performed qualifying service by substituting ''2 years after the effective date under section 603(g) of the Intelligence Authorization Act for Fiscal Year 2022'' for ''30 years after the death or other event which gives rise to title to the benefit''.

(g) EFFECTIVE DATE.—This section shall take effect on the date that is 30 days after the date of the enactment of this Act.

SEC. 604. ACCESS BY COMPTROLLER GENERAL OF THE UNITED STATES TO CERTAIN CYBERSECURITY RECORDS.

Section 5710 of the National Defense Authorization Act for Fiscal Year 2020 (2 U.S.C. 4111) is amended—

(1) by redesignating subsection (d) as subsection (e);

(2) by inserting after subsection (c) the following:

''(d) RIGHT OF ACCESS.—Notwithstanding any other provision of law, for the purpose of preparing each report required by subsection (a), the Comptroller General may obtain from the Architect of the Capitol, the Congressional Budget Office, the Library of Congress, the Office of Congressional Workplace Rights, the Sergeant at Arms and Doorkeeper of the Senate, the Sergeant at Arms of the House of Representatives, the Chief Administrative Officer of the House of Representatives, the Secretary of the Senate, and the United States Capitol Police, and any contractor of any such entity, such records as the Comptroller General may require to prepare the report.''; and

(3) by adding at the end the following:

''(f) RELATIONSHIP TO EXISTING AUTHORITY.—Nothing in this section shall be construed to limit, amend, supersede, or restrict in any manner any authority of the Comptroller General, except as specifically provided for in subsection (d).''.

SEC. 605. REPORTS ON INTELLIGENCE SUPPORT FOR AND CAPACITY OF THE SERGEANTS AT ARMS OF THE SENATE AND THE HOUSE OF REPRESENTATIVES AND THE UNITED STATES CAPITOL POLICE.

(a) DEFINITIONS.—In this section:

(1) RELEVANT CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term ''relevant congressional intelligence committees'' means—

(A) the Select Committee on Intelligence, the Committee on Rules and Administration, the Committee on Appropriations, and the Committee on the Judiciary of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on House Administration, the Committee on Appropriations, and the Committee on the Judiciary of the House of Representatives.

(2) SERGEANTS AT ARMS.—The term ''Sergeants at Arms'' means the Sergeant at Arms and

Doorkeeper of the Senate and the Sergeant at Arms of the House of Representatives.

(b) REPORT ON INTELLIGENCE SUPPORT.—

(1) REPORT REQUIRED.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Director of the Federal Bureau of Investigation and the Secretary of Homeland Security, shall submit to the relevant congressional intelligence committees a report on intelligence support provided to the Sergeants at Arms and the United States Capitol Police.

(2) ELEMENTS.—The report required by paragraph (1) shall include a description of the following:

(A) Policies related to the Sergeants at Arms and the United States Capitol Police as customers of intelligence.

(B) How the intelligence community, the Federal Bureau of Investigation, and the Department of Homeland Security, including the Cybersecurity and Infrastructure Security Agency, are structured, staffed, and resourced to provide intelligence support to the Sergeants at Arms and the United States Capitol Police.

(C) The classified electronic and telephony interoperability of the intelligence community, the Federal Bureau of Investigation, and the Department of Homeland Security with the Sergeants at Arms and the United States Capitol Police.

(D) Any expedited security clearances provided for the Sergeants at Arms and the United States Capitol Police.

(E) Counterterrorism intelligence and other intelligence relevant to the physical security of Congress that are provided to the Sergeants at Arms and the United States Capitol Police, including—

(i) strategic analysis and real-time warning; and

(ii) access to classified systems for transmitting and posting intelligence.

(F) Cyber intelligence relevant to the protection of cyber networks of Congress and the personal devices and accounts of Members and employees of Congress, including—

(i) strategic and real-time warnings, such as malware signatures and other indications of attack; and

(ii) access to classified systems for transmitting and posting intelligence.

(3) FORM.—The report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(c) GOVERNMENT ACCOUNTABILITY OFFICE REPORT.—

(1) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the relevant congressional intelligence committees a report on the capacity of the Sergeants at Arms and the United States Capitol Police to access and use intelligence and threat information relevant to the physical and cyber security of Congress.

(2) ELEMENTS.—The report required by paragraph (1) shall include the following:

(A) An assessment of the extent to which the Sergeants at Arms and the United States Capitol Police have the resources, including facilities, cleared personnel, and necessary training, and authorities to adequately access, analyze, manage, and use intelligence and threat information necessary to defend the physical and cyber security of Congress.

(B) The extent to which the Sergeants at Arms and the United States Capitol Police communicate and coordinate threat data with each other and with other local law enforcement entities.

(3) FORM.—The report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

SEC. 606. STUDY ON VULNERABILITY OF GLOBAL POSITIONING SYSTEM TO HOSTILE ACTIONS.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services, the Committee on Science, Space, and Technology, and the Committee on Appropriations of the House of Representatives.

(b) STUDY REQUIRED.—The Director of National Intelligence shall, in consultation with the Secretary of Defense and the Secretary of Commerce, conduct a study on

the vulnerability of the Global Positioning System (GPS) to hostile actions, as well as any actions being undertaken by the intelligence community, the Department of Defense, the Department of Commerce, and any other elements of the Federal Government to mitigate any risks stemming from the potential unavailability of the Global Positioning System.

(c) ELEMENTS.—The study conducted under subsection (b) shall include net assessments and baseline studies of the following:

(1) The vulnerability of the Global Positioning System to hostile actions.

(2) The potential negative effects of a prolonged Global Positioning System outage, including with respect to the entire society, to the economy of the United States, and to the capabilities of the Armed Forces.

(3) Alternative systems that could back up or replace the Global Positioning System, especially for the purpose of providing positioning, navigation, and timing, to United States civil, commercial, and government users.

(4) Any actions being planned or undertaken by the intelligence community, the Department of Defense, the Department of Commerce, and other ele-

ments of the Federal Government to mitigate any risks to the entire society, to the economy of the United States, and to the capabilities of the Armed Forces, stemming from a potential unavailability of the Global Positioning System.

(d) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a report in writing and provide such committees a briefing on the findings of the Director with respect to the study conducted under subsection (b).

SEC. 607. AUTHORITY FOR TRANSPORTATION OF FEDERALLY OWNED CANINES ASSOCIATED WITH FORCE PROTECTION DUTIES OF INTELLIGENCE COMMUNITY.

Section 1344(a)(2)(B) of title 31, United States Code, is amended by inserting ", or transportation of federally owned canines associated with force protection duties of any part of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003))" after "duties".

Calendar No. 116

117TH CONGRESS
1ST SESSION

S. 2610

A BILL

To authorize appropriations for fiscal year 2022 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

AUGUST 4, 2021

Read twice and placed on the calendar

From	"(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @dodig.mil>
Cc	"(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>
Subject	Notes on the WARs - 8/27
Date	Fri, 27 Aug 2021 20:19:03 +0000
Message-Id	<a5188c706ae24f39baf0c0bbc61813cb@DODIG.MIL>

~~Contains CUI.~~

Gents,

Have a great weekend.

AI: NSTR.

Audit: (b) (5), (b) (6) .

(b) (5), (b) (6) .

DIEM: (b) (5), (b) (6)

(b) (5) .

EVAL: (b) (5) .

Evaluation of the DoD's Actions Regarding the Unidentified Aerial Phenomena. (b) (5) .

INV: (b) (5), (b) (6) .

(b) (5) .

OCO:

(~~CUI~~) (b) (5) [redacted]

- (b) (5), (b) (6) [redacted]
- (b) (5), (b) (6) [redacted].

(~~CUI~~) (b) (5) [redacted].

MST: (b) (5) [redacted]

(~~CUI~~) (b) (5) [redacted]

(b) (6) [redacted].

(b) (5) [redacted].

OGC:

(b) (5), (b) (6) [redacted].

(b) (5), (b) (6) [redacted]

(~~CUI~~) (b) (5), (b) (6) [redacted]

(b) (5) [redacted]

(b) (5), (b) (6)

OLAC:

~~(U)~~ (b) (5), (b) (6)

(b) (5)

~~(CUI) (CUI)~~ (b) (5), (b) (6)

OPR: (b) (5)

(b) (5)

(b) (5)

(b) (5), (b) (6) .

EEOO: (b) (5) .

~~Contains CUI~~

From	'(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>
To	List SESLIST <(b) (6) @dodig.mil>
Cc	"Zola, Michael C., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) ., OIG DoD" <(b) (6) @DODIG.MIL>
Subject	H.R. 5412 - FY22 Intelligence Authorization Act (HPSCI)
Date	Wed, 6 Oct 2021 16:15:04 +0000
Message-Id	<a7abb66807b245cf9f109172938c2d3c@DODIG.MIL>

Good afternoon,
Attached please find the HPSCI version of the FY 2022 Intelligence Authorization bill.
(b) (5)
.
The bill also contains language requiring the CIA IG to conduct a review related to anomalous health incidents, requires a National Intelligence Estimate on threats and opportunities arising out of Afghanistan in the next two years, includes a detailed provision that addresses intelligence gaps and sharpens America's focus on transnational white supremacist extremist threats, imposes a requirement of certain former intelligence officers to report employment with a foreign government, and mandates intelligence sharing with the Department of Defense's UAP task force.

Below is press release for the HPSCI, which provides a more detailed summary of the bill:
Chairman Schiff Applauds Passage of 2022 Intelligence Authorization Act
Today, the House Intelligence Committee approved the Fiscal Year 2022 Intelligence Authorization Act through a bipartisan voice vote, authorizing funding for comprehensive congressional oversight of the Intelligence Community. The measure ensures the protection of civil liberties, provides care for our personnel, and authorizes the resources intelligence professionals need to safeguard national security.
"One of our committee's principal responsibilities is crafting an Intelligence Authorization Act that keeps our country secure while ensuring the Congress' ability to conduct vigorous oversight, protect civil l berties, care f or our personnel, and provide for the resources intelligence professionals need to safeguard national security," said Schiff. "The bill passed out of the committee today is a strong bipartisan package, and I would like to tha nk all of our Members and staff on both sides of the aisle for working diligently to contribute to and shape this legislation. I am particularly pleased by the significant progress made within this authorization act to provide improved care for members of the IC, particularly those impacted by anomalous health incidents, to protect against future pandemics and global health threats, and to further our pivot towards hard targets and the great power competition we face from China and Russia. I hope that the full House will be able to take up this legislation soon as we continue the process of enacting these reforms into law."
This year's IAA authorizes funding for the IC at roughly 0.5% above the President's FY 2022 Budget Request. The legislation advances significant bipartisan Committee priorities, including:

Caring for Victims of Anomalous Health Incidents. The bill includes provisions arising out of HPSCI's thorough oversight of the Intelligence Community's response to Anomalous Health Incidents, which have affected numerous IC officers and government employees, their spouses, and children.
Most significantly, the bill contains a provision requiring the president to develop uniform protocols for comprehensive pre-deployment testing of individuals and comprehensive treatment and care of individuals, and their families, following an AHI. The bill also requires the creation of protocols that encourage the reporting of

AHIs and for handling complaints or concerns regarding the government's treatment of employees who report an AHI.

Taken together, these provisions will cause significant improvements throughout the U.S. government in standardizing and ensuring quality care for government officials who experience an anomalous health incident. For the CIA, specifically, the title will ensure that OMS provides the highest standard of care to CIA officers in all of OMS' activities, including when a CIA officer experiences an AHI.

Getting Ready for the Next Pandemic. The bill takes several steps to put the IC in a stronger position to face the next pandemic. The bill substantially enhances the authorities of the National Counterproliferation Center to address the full spectrum of foreign biological threats and to provide indications and warnings about emerging biological threats. The bill also includes a report assessing the value of adding the Department of Health and Human Services Office of National Security to the Intelligence Community, as well as mandating additional reporting about the IC's posture against foreign biological threats of all kinds. The classified annex includes several provisions about pandemic preparedness and global health security.

Afghanistan - Looking Forward. The bill requires a National Intelligence Estimate - the IC's premier analytic product - on threats and opportunities arising out of Afghanistan in the next two years, including relations between the Taliban and China, Iran, Pakistan, and Russia, the Taliban's approach to human rights, and the safety and ability to secure safe transit of Afghan allies of the United States. The bill also requires a detailed report on our current ability to collect intelligence regarding Afghanistan, including detection and prevention of any increased threats to the homeland, and an assessment of how to improve our capabilities following U.S. withdrawal.

China and Counterintelligence. The bill requires the FBI's counterintelligence division to conduct a security assessment of any Chinese-origin product or service before the FBI procures such product or service. Another provision calls for a report on cooperation between China and the UAE regarding defense, security, technology, and other matters.

Understanding Transnational White Supremacy. The bill includes a detailed provision that addresses intelligence gaps and sharpens America's focus on transnational white supremacist extremist threats. Specifically, this bill will improve federal intelligence agencies' ability to prioritize white supremacist extremist threats, including ties to international groups and their finances. It mandates that the National Counterterrorism Center - alongside the Federal Bureau of Investigation and the Department of Homeland Security - explore and analyze more thoroughly the ideology and objectives driving white supremacist groups with transnational connections, including their leadership and operational structure.

Restricting Former Intelligence Officers from Misusing Their Skills. The bill imposes a requirement that certain former intelligence officers, who occupied particularly sensitive positions, report employment with a foreign government related to national security, intelligence, or internal security. It also bars such employment for 30 months after working in the IC. The provision includes criminal penalties for those who do not follow the provision, including violating cooling-off period, failing to report employment with a foreign government, or falsifying their reports. The intention of the provision is to discourage former IC employees from providing intelligence services to adversaries or to countries with poor human rights records.

Promoting Human Rights. Several provisions advance the Committee's longstanding interest in protecting and promoting human rights. One provision will help the committee understand how the IC prioritizes enforcing human rights sanctions under current law such as the Global Magnitsky Sanctions and the Khashoggi Ban. Another provision requires reports on cyber vulnerabilities acquired by the IC and on certain foreign commercial providers of cyber vulnerabilities whose services can be used to violate human rights.

Detecting and Monitoring Wildfires in the U.S. The bill requires that the National Geospatial Intelligence Agency lead a coordinated, interagency review with the Department of Defense, and the organizations within the National Interagency Fire Center, to assess existing technical capabilities and future opportunities to detect and monitor wildfires. This measure ensures the government is leveraging all possible resources, within existing authorities, to provide timely and accurate information to firefighters fighting wildfires, including those in the Western U.S. Those fires are becoming increasingly common and severe because of climate change.

Great Power Competition in the 'Gray Zone'. The United States is facing new forms of competition and threats from adversaries using tactics that fall on a spectrum between ordinary statecraft and open warfare. The bill contains a provision mandating a National Intelligence Estimate that uses the IC's classified reporting to describe how foreign adversaries use gray zone activities to advance their interests and assess what U.S. responses would cause our adversaries to escalate - or deescalate - that activity.

Protecting IC Employees. A provision will seek information on cases in which the DIA inspector general substantiated claims of reprisal or abuse of authority against DIA managers, and how the resulting disciplinary decisions were made. It also reinforces the critical need for IG independence from agency leadership. The effect

is to ensure that employees at that agency are having their allegations fully and thoroughly investigated and senior leaders and managers at all levels are held accountable for their actions.
Shining a Light on Saudi Extremism. The bill requires that the Director of National Intelligence prepare a detailed report on the threat of extremist ideologies propagated from Saudi Arabia and the failure of the Government of Saudi Arabia to prevent the propagation of such ideologies.
Persistent Pursuit of Unexplained Aerial Phenomena. Following a bipartisan oversight hearing on Unexplained Aerial Phenomena, the bill is carrying a bicameral provision mandating intelligence sharing with the Department of Defense's UAP task force. The provision will ensure that the task force will be able to fully draw on all classified reporting about UAPs as they continue to investigate this mysterious threat to U.S. airspace and our military forces.

Thanks,
(b) (6)
Office of Legislative Affairs and Communications
DoD Office of Inspector General
(b) (6)
Visit www.dodig.mil
Sign up for DoD IG reports, project announcements and our monthly newsletter: http://www.dodig.mil/Mailing-Lists/

.....

Attachment Name : iaa22_ans_xml.pdf

AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 5412 OFFERED BY MR. SCHIFF OF CALIFORNIA

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Intelligence Authorization Act for Fiscal Year 2022''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—INTELLIGENCE ACTIVITIES

Sec. 101. Authorization of appropriations.
Sec. 102. Classified schedule of authorizations.
Sec. 103. Intelligence community management account.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Sec. 201. Authorization of appropriations.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

Sec. 301. Restriction on conduct of intelligence activities.
Sec. 302. Increase in employee compensation and benefits authorized by law.
Sec. 303. Temporary authority for paid leave for a serious health condition.
Sec. 304. Harmonization of whistleblower protections.
Sec. 305. Congressional oversight of certain special access programs.
Sec. 306. Clarification of requirement for authorization of funding for intelligence activities.
Sec. 307. Authorization of support by Director of National Intelligence for certain activities relating to intelligence community workforce.
Sec. 308. Requirements for certain employment activities by former intelligence officers and employees.

Sec. 309. Non-reimbursable detail of intelligence community personnel to assist with processing and resettlement of refugees, parolees, and other aliens from Afghanistan.
Sec. 310. Authority for transport of certain canines associated with force protection duties of intelligence community.
Sec. 311. Development of definitions for certain terms relating to intelligence.
Sec. 312. Support for and oversight of Unidentified Aerial Phenomena Task Force.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

Sec. 401. National Counterproliferation and Biosecurity Center.
Sec. 402. Clarification of certain responsibility of the Director of National Intelligence.
Sec. 403. Responsibility of Director of National Intelligence regarding National Intelligence Program budget concerning Federal Bureau of Investigation.
Sec. 404. Climate Security Advisory Council.

Subtitle B—Other Elements

Sec. 411. Protection of certain facilities and assets of Central Intelligence Agency from unmanned aircraft.
Sec. 412. Modification of National Geospatial-Intelligence Agency personnel management authority to attract experts in science and engineering.
Sec. 413. Requirements for termination of dual-hat arrangement for Commander of the United States Cyber Command.
Sec. 414. National Space Intelligence Center.
Sec. 415. Procurement by Federal Bureau of Investigation of Chinese products and services.
Sec. 416. Counterintelligence units at non-intelligence community Federal departments and agencies.
Sec. 417. Detection and monitoring of wildfires.

TITLE V—ANOMALOUS HEALTH INCIDENTS AND OTHER HEALTH CARE MATTERS

Sec. 501. Compensation and professional standards for certain medical officers of the Central Intelligence Agency.
Sec. 502. Medical advisory board of the Central Intelligence Agency.
Sec. 503. Report on protocols for certain intelligence community employees and dependents.
Sec. 504. Inspector General of the Central Intelligence Agency review of Office of Medical Services.
Sec. 505. Clarification of effect of certain benefits relating to injuries to the brain.

TITLE VI—MATTERS RELATING TO FOREIGN COUNTRIES

Sec. 601. National Intelligence Estimate on security situation in Afghanistan and related region.
Sec. 602. Report on likelihood of military action by countries of the South Caucasus.

Sec. 603. Report on intelligence collection posture and other matters relating to Afghanistan and related region.
Sec. 604. Report on threat posed by emerging Chinese technology companies.
Sec. 605. Report on cooperation between China and United Arab Emirates.
Sec. 606. Report on propagation of extremist ideologies from Saudi Arabia.
Sec. 607. Report on effects of sanctions by United States.

TITLE VII—REPORTS AND OTHER MATTERS

Sec. 701. Pilot program for security vetting of certain individuals.
Sec. 702. Intelligence assessment and reports on foreign racially motivated violent extremists.
Sec. 703. Periodic report on positions in the intelligence community that can be conducted without access to classified information, networks, or facilities.
Sec. 704. Biennial reports on foreign biological threats.
Sec. 705. Annual reports on domestic activities of the intelligence community.
Sec. 706. Annual reports on certain cyber vulnerabilities procured by intelligence community and foreign commercial providers of cyber vulnerabilities.
Sec. 707. Improvements to annual report on demographic data of employees of intelligence community.
Sec. 708. National Intelligence Estimate on escalation and de-escalation of gray zone activities in great power competition.
Sec. 709. Report on certain actions taken by intelligence community with respect to human rights and international humanitarian law.
Sec. 710. Briefing on trainings relating to blockchain technology.
Sec. 711. Report on prospective ability to administer COVID–19 vaccines and other medical interventions to certain intelligence community personnel.
Sec. 712. Report on potential inclusion within intelligence community of the Office of National Security of the Department of Health and Human Services.
Sec. 713. Reports relating to Inspector General of Defense Intelligence Agency.
Sec. 714. Report on rare earth elements.
Sec. 715. Report on plan to fully fund the Information Systems Security Program and next generation encryption.
Sec. 716. Review of National Security Agency and United States Cyber Command.

SEC. 2. DEFINITIONS.

In this Act:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term ''congressional intelligence committees'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(2) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 2022 for the conduct of the intelligence and intelligence-related activities of the following elements of the United States Government:

(1) The Office of the Director of National Intelligence.

(2) The Central Intelligence Agency.

(3) The Department of Defense.

(4) The Defense Intelligence Agency.

(5) The National Security Agency.

(6) The Department of the Army, the Department of the Navy, and the Department of the Air Force.

(7) The Coast Guard.

(8) The Department of State.

(9) The Department of the Treasury.

(10) The Department of Energy.

(11) The Department of Justice.

(12) The Federal Bureau of Investigation.

(13) The Drug Enforcement Administration.

(14) The National Reconnaissance Office.

(15) The National Geospatial-Intelligence Agency.

(16) The Department of Homeland Security.

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

(a) SPECIFICATIONS OF AMOUNTS.—The amounts authorized to be appropriated under section 101 for the conduct of the intelligence activities of the elements listed in paragraphs (1) through (16) of section 101, are those specified in the classified Schedule of Authorizations prepared to accompany this Act.

(b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AUTHORIZATIONS.—

(1) AVAILABILITY.—The classified Schedule of Authorizations referred to in subsection (a) shall be made available to the Committee on Appropriations of the Senate, the Committee on Appropriations of the House of Representatives, and to the President.

(2) DISTRIBUTION BY THE PRESIDENT.—Subject to paragraph (3), the President shall provide for suitable distribution of the classified Schedule of Authorizations referred to in subsection (a), or of ap-

propriate portions of such Schedule, within the executive branch.

(3) LIMITS ON DISCLOSURE.—The President shall not publicly disclose the classified Schedule of Authorizations or any portion of such Schedule except—

(A) as provided in section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 3306(a));

(B) to the extent necessary to implement the budget; or

(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2022 the sum of $619,000,000.

(b) CLASSIFIED AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2022 such additional amounts as are

specified in the classified Schedule of Authorizations referred to in section 102(a).

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund $514,000,000 for fiscal year 2022.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

SEC. 301. RESTRICTION ON CONDUCT OF INTELLIGENCE ACTIVITIES.

The authorization of appropriations by this Act shall not be deemed to constitute authority for the conduct of any intelligence activity which is not otherwise authorized by the Constitution or the laws of the United States.

SEC. 302. INCREASE IN EMPLOYEE COMPENSATION AND BENEFITS AUTHORIZED BY LAW.

Appropriations authorized by this Act for salary, pay, retirement, and other benefits for Federal employees may be increased by such additional or supplemental amounts

as may be necessary for increases in such compensation or benefits authorized by law.

SEC. 303. TEMPORARY AUTHORITY FOR PAID LEAVE FOR A SERIOUS HEALTH CONDITION.

(a) AUTHORIZATION OF PAID LEAVE FOR A SERIOUS HEALTH CONDITION FOR EMPLOYEES OF ELEMENTS OF THE INTELLIGENCE COMMUNITY.—

(1) IN GENERAL.—Title III of the National Security Act of 1947 (50 U.S.C. 3071 et seq.) is amended by inserting after section 304 the following:

"SEC. 305. TEMPORARY AUTHORITY FOR PAID LEAVE FOR A SERIOUS HEALTH CONDITION.

''(a) DEFINITIONS.—In this section:

''(1) PAID SERIOUS HEALTH CONDITION LEAVE.—The term 'paid serious health condition leave' means paid leave taken under subsection (b).

''(2) SERIOUS HEALTH CONDITION.—The term 'serious health condition' has the meaning given the term in section 6381 of title 5, United States Code.

''(3) SON OR DAUGHTER.—The term 'son or daughter' has the meaning given the term in section 6381 of title 5, United States Code.

''(b) PAID SERIOUS HEALTH CONDITION LEAVE.—During the period specified in subsection (f), and notwith-

standing any other provision of law, a civilian employee of an element of the intelligence community shall have available a total of 12 administrative workweeks of paid leave during any 12-month period for one or more of the following:

''(1) In order to care for the spouse, or a son, daughter, or parent, of the employee, if such spouse, son, daughter, or parent has a serious health condition.

''(2) Because of a serious health condition that makes the employee unable to perform the functions of the employee's position.

''(c) TREATMENT OF SERIOUS HEALTH CONDITION LEAVE REQUEST.—Notwithstanding any other provision of law, an element of the intelligence community shall accommodate an employee's leave schedule request under subsection (b), including a request to use such leave intermittently or on a reduced leave schedule, to the extent that the requested leave schedule does not unduly disrupt agency operations.

''(d) RULES RELATING TO PAID LEAVE.—During the period specified in subsection (f), and notwithstanding any other provision of law—

''(1) an employee of an element of the intelligence community—

"(A) shall be required to first use all accrued or accumulated paid sick leave before being allowed to use paid serious health condition leave; and

"(B) may not be required to first use all or any portion of any unpaid leave available to the employee before being allowed to use paid serious health condition leave; and

"(2) paid serious health condition leave—

"(A) shall be payable from any appropriation or fund available for salaries or expenses for positions within the employing element;

"(B) may not be considered to be annual or vacation leave for purposes of section 5551 or 5552 of title 5, United States Code, or for any other purpose;

"(C) if not used by the employee before the end of the 12-month period described in subsection (b) to which the leave relates, may not be available for any subsequent use and may not be converted into a cash payment;

"(D) may be granted only to the extent that the employee does not receive a total of more than 12 weeks of paid serious health condition leave in any 12-month period;

"(E) shall be used in increments of hours (or fractions thereof), with 12 administrative workweeks equal to 480 hours for employees of elements of the intelligence community with a regular full-time work schedule and converted to a proportional number of hours for employees of such elements with part-time, seasonal, or uncommon tours of duty; and

"(F) may not be used during off-season (nonpay status) periods for employees of such elements with seasonal work schedules.

"(e) IMPLEMENTATION.—

"(1) CONSISTENCY WITH SERIOUS HEALTH CONDITION LEAVE UNDER TITLE 5.—The Director of National Intelligence shall carry out this section in a manner consistent, to the extent appropriate, with the administration of leave taken under section 6382 of title 5, United States Code, for a reason described in subparagraph (C) or (D) of subsection (a)(1) of that section, including with respect to the authority to require a certification described in section 6383 of such title.

"(2) IMPLEMENTATION PLAN.—Not later than 1 year after the date of enactment of this section, the Director of National Intelligence shall submit to

the congressional intelligence committees an implementation plan that includes—

"(A) processes and procedures for implementing the paid serious health condition leave policies under subsections (b) through (d) during the period specified in subsection (f);

"(B) an explanation of how such implementation will be reconciled with policies of other elements of the Federal Government, including the impact on elements funded by the National Intelligence Program that are housed within agencies outside the intelligence community;

"(C) the projected impact of such implementation on the workforce of the intelligence community, including take rates, retention, recruiting, and morale, broken down by each element of the intelligence community; and

"(D) all costs or operational expenses associated with such implementation.

"(3) DIRECTIVE.—Not later than 90 days after the Director of National Intelligence submits the implementation plan under paragraph (2), the Director of National Intelligence shall issue a written direc-

tive to implement this section, which directive shall take effect on the date of issuance.

''(f) DURATION OF AUTHORITY.—The authority and requirements under subsections (b) through (d) shall only apply during the 3-year period beginning on the date on which the Director of National Intelligence issues the written directive under subsection (e)(3).

''(g) ANNUAL REPORT.—During the period specified in subsection (f), the Director of National Intelligence shall submit to the congressional intelligence committees an annual report that—

''(1) details the number of employees of each element of the intelligence community who applied for and took paid serious health condition leave during the year covered by the report;

''(2) includes updates on major implementation challenges or costs associated with paid serious health condition leave; and

''(3) includes a recommendation of the Director with respect to whether to extend the period specified in subsection (f).''.

(2) CLERICAL AMENDMENT.—The table of contents at the beginning of such Act is amended by inserting after the item relating to section 304 the following:

''Sec. 305. Paid serious health condition leave.''.

(b) APPLICABILITY.—Section 305 of the National Security Act of 1947, as added by subsection (b), shall apply with respect to leave taken in connection with a serious health condition (as defined in subsection (a) of such section 305) that occurs or continues to exist during the period specified in subsection (f) of such section.

SEC. 304. HARMONIZATION OF WHISTLEBLOWER PROTECTIONS.

(a) PROHIBITED PERSONNEL PRACTICES IN THE INTELLIGENCE COMMUNITY.—

(1) THREATS RELATING TO PERSONNEL ACTIONS.—

(A) AGENCY EMPLOYEES.—Section 1104(b) of the National Security Act of 1947 (50 U.S.C. 3234(b)) is amended, in the matter preceding paragraph (1)—

(i) by striking ''Any employee of an agency'' and insert ''Any employee of a covered intelligence community element or an agency''; and

(ii) by inserting '', or threaten to take or fail to take,'' after ''take or fail to take''.

(B) CONTRACTOR EMPLOYEES.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1))

is amended, in the matter preceding subparagraph (A), by inserting ", or threaten to take or fail to take," after "take or fail to take".

(2) PROTECTION FOR CONTRACTOR EMPLOYEES AGAINST REPRISAL FROM AGENCY EMPLOYEES.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1)), as amended by paragraph (1)(B) of this subsection, is further amended, in the matter preceding subparagraph (A), by inserting "of an agency or" after "Any employee".

(3) ENFORCEMENT.—Subsection (d) of section 1104 of such Act (50 U.S.C. 3234) is amended to read as follows:

"(d) ENFORCEMENT.—The President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.".

(b) RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.—

(1) ENFORCEMENT.—Section 3001(j) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)) is amended—

(A) by redesignating paragraph (8) as paragraph (9); and

(B) by inserting after paragraph (7) the following:

''(8) ENFORCEMENT.—Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.''.

(2) TOLLING OF DEADLINE FOR APPEAL OF PROHIBITED REPRISAL.—Section 3001(j)(4) of such Act (50 U.S.C. 3341(j)(4)) is amended—

(A) in subparagraph (A), by inserting ''(except as provided by subparagraph (D))'' after ''within 90 days''; and

(B) by adding at the end the following new subparagraph:

''(D) TOLLING.—The time requirement established by subparagraph (A) for an employee or former employee to appeal the decision of an agency may be tolled if the employee or former employee presents substantial credible evidence showing why the employee or former employee did not timely initiate the appeal and why the enforcement of the time requirement would be

unfair, such as evidence showing that the employee or former employee—

"(i) did not receive notice of the decision; or

"(ii) could not timely initiate the appeal because of factors beyond the control of the employee or former employee.".

(c) CORRECTION OF DEFINITION OF AGENCY.—Section 3001(a)(1)(B) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(a)(1)(B)) is amended by striking "and" and inserting "or".

(d) ESTABLISHING CONSISTENCY WITH RESPECT TO PROTECTIONS FOR DISCLOSURES OF MISMANAGEMENT.—

(1) SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—Section 3001(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)) is amended—

(A) in subparagraph (A)(ii), by striking "gross mismanagement" and inserting "mismanagement"; and

(B) in subparagraph (B)(ii), by striking "gross mismanagement" and inserting "mismanagement".

(2) PERSONNEL ACTIONS AGAINST CONTRACTOR EMPLOYEES.—Section 1104(c)(1)(B) of the National Security Act of 1947 (50 U.S.C. 3234(c)(1)(B)) is amended by striking ''gross mismanagement'' and inserting ''mismanagement''.

(e) PROTECTED DISCLOSURES TO SUPERVISORS.—

(1) PERSONNEL ACTIONS.—

(A) DISCLOSURES BY AGENCY EMPLOYEES TO SUPERVISORS.—Section 1104(b) of the National Security Act of 1947 (50 U.S.C. 3234(b)), as amended by subsection (a)(1)(A), is further amended, in the matter preceding paragraph (1), by inserting ''a supervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including'' before ''the head of the employing agency''.

(B) DISCLOSURES BY CONTRACTOR EMPLOYEES TO SUPERVISORS.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1)), as amended by subsection (a), is further amended, in the matter preceding subparagraph (A), by inserting ''a supervisor in the contractor employee's direct chain of command, or a su-

pervisor of the contracting agency with responsibility for the subject matter of the disclosure, up to and including'' before ''the head of the contracting agency''.

(2) SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—Section 3001(j)(1)(A) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)(A)) is amended, in the matter preceding clause (i), by inserting ''a supervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including'' before ''the head of the employing agency''.

(f) ESTABLISHING PARITY FOR PROTECTED DISCLOSURES.—Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is further amended—

(1) in subsection (b), as amended by subsections (a)(1)(A) and (e)(1)(A)—

(A) by redesignating paragraphs (1) and (2) as subparagraphs (A) and (B), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the right;

(B) in the matter preceding subparagraph (A), as redesignated and moved by subpara-

graph (B) of this paragraph, by striking ''for a lawful disclosure'' and inserting the following: ''for—

''(1) any lawful disclosure''; and

(C) by adding at the end the following:

''(2) any lawful disclosure that complies with—

''(A) subsections (a)(1), (d), and (g) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);

''(B) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or

''(C) subparagraphs (A), (D), and (I) of section 103H(k)(5); or

''(3) if the actions do not result in the employee unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

''(A) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

''(B) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in subparagraph (A); or

"(C) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General."; and

(2) in subsection (c)(1), as amended by subsections (a) and (e)(1)(B)—

(A) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively, and moving such clauses, as so redesignated, 2 ems to the right;

(B) in the matter preceding clause (i), as redesignated and moved by subparagraph (B) of this paragraph, by striking "for a lawful disclosure" and inserting the following: "for—

"(A) any lawful disclosure"; and

(C) by adding at the end the following:

"(B) any lawful disclosure that complies with—

"(i) subsections (a)(1), (d), and (g) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);

"(ii) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or

"(iii) subparagraphs (A), (D), and (I) of section 103H(k)(5); or

"(C) if the actions do not result in the contractor employee unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

"(i) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

"(ii) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in clause (i); or

"(iii) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.".

(g) CLARIFICATION RELATING TO PROTECTED DISCLOSURES.—Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is further amended—

(1) by redesignating subsections (d) and (e) as subsections (f) and (g), respectively; and

(2) by inserting after subsection (c) the following:

''(d) RULE OF CONSTRUCTION.—Consistent with the protection of sources and methods, nothing in subsection (b) or (c) shall be construed to authorize—

''(1) the withholding of information from Congress; or

''(2) the taking of any personnel action against an employee who lawfully discloses information to Congress.

''(e) DISCLOSURES.—A disclosure shall not be excluded from this section because—

''(1) the disclosure was made to an individual, including a supervisor, who participated in an activity that the employee reasonably believed to be covered under subsection (b)(1)(B) or the contractor employee reasonably believed to be covered under subsection (c)(1)(A)(ii);

''(2) the disclosure revealed information that had been previously disclosed;

''(3) the disclosure was not made in writing;

''(4) the disclosure was made while the employee was off duty;

''(5) of the amount of time which has passed since the occurrence of the events described in the disclosure; or

''(6) the disclosure was made during the normal course of duties of an employee or contractor employee.''.

(h) CORRECTION RELATING TO NORMAL COURSE DISCLOSURES.—Section 3001(j)(3) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(3)) is amended—

(1) by striking ''DISCLOSURES.—'' and all that follows through ''because—'' and inserting ''DISCLOSURES.—A disclosure shall not be excluded from paragraph (1) because—'';

(2) by striking subparagraph (B);

(3) by redesignating clauses (i) through (v) as subparagraphs (A) through (E), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the left;

(4) in subparagraph (D), as so redesignated, by striking ''or'' at the end;

(5) in subparagraph (E), as redesignated by paragraph (3), by striking the period at the end and inserting ''; or''; and

(6) by adding at the end the following:

"(F) the disclosure was made during the normal course of duties of an employee.".

(i) CLARIFICATION RELATING TO RULE OF CONSTRUCTION.—Section 3001(j)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(2)) is amended by inserting "or clearance action" after "personnel action".

(j) CLARIFICATION RELATING TO PROHIBITED PRACTICES.—Section 3001(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)), as amended by this section, is further amended by striking "over" and inserting "to take, direct others to take, recommend, or approve".

(k) TECHNICAL CORRECTION.—Section 3001(j)(1)(C)(i) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)(C)(i)) is amended by striking "(h)" and inserting "(g)".

(l) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community shall submit to the congressional intelligence committees a report assessing the extent to which protections provided under Presidential Policy Directive 19 (relating to protecting whistleblowers with access to classified information) have been codified in statutes.

SEC. 305. CONGRESSIONAL OVERSIGHT OF CERTAIN SPECIAL ACCESS PROGRAMS.

(a) IN GENERAL.—Title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) is amended by inserting after section 501 the following new section (and conforming the table of contents at the beginning of such Act accordingly):

"SEC. 501A. CONGRESSIONAL OVERSIGHT OF CERTAIN SPECIAL ACCESS PROGRAMS.

"(a) REPORTS AND NOTIFICATIONS.—At the same time that the Secretary of Defense submits any report or notification under section 119 of title 10, United States Code, that relates to a covered special access program or a new covered special access program, the Secretary shall also submit such report or notification to the congressional intelligence committees.

"(b) BRIEFINGS.—On a periodic basis, but not less frequently than semiannually, the Secretary of Defense shall provide to the chairmen and ranking minority members of the congressional intelligence committees, and to any staff of such a committee designated by either the chair or ranking member for purposes of this subsection, a briefing on covered special access programs. Each such briefing shall include, at a minimum—

"(1) a description of the activity of the program during the period covered by the briefing; and

"(2) documentation with respect to how the program has achieved outcomes consistent with requirements documented by the Director of National Intelligence and the Secretary of Defense.

"(c) NOTIFICATIONS ON COMPARTMENTS AND SUBCOMPARTMENTS.—

"(1) REQUIREMENT.—Except as provided by paragraph (2), a head of an element of the intelligence community may not establish a compartment or a subcompartment under a covered special access program until the head notifies the congressional intelligence committees of such compartment or subcompartment, as the case may be.

"(2) WAIVER.—

"(A) DETERMINATION.—On a case-by-case basis, the Director of National Intelligence may waive the requirement under paragraph (1). Not later than two days after making such a waiver, the Director shall notify the congressional intelligence committees of the waiver, including a justification for the waiver.

"(B) SUBMISSION.—Not later than 30 days after the date on which the Director makes a waiver under subparagraph (A), the head of the element of the intelligence commu-

nity for whom the waiver was made shall submit to the congressional intelligence committees the notification required under paragraph (1) relating to such waiver.

''(d) ANNUAL REPORTS.—

''(1) REQUIREMENT.—On an annual basis, the head of each element of the intelligence community shall submit to the congressional intelligence committees a report on covered special access programs administered by the head.

''(2) MATTERS INCLUDED.—Each report shall include, with respect to the period covered by the report, the following:

''(A) A list of all compartments and subcompartments of covered special access programs active as of the date of the report.

''(B) A list of all compartments and subcompartments of covered special access programs terminated during the period covered by the report.

''(C) With respect to the report submitted by the Director of National Intelligence, in addition to the matters specified in subparagraphs (A) and (B)—

"(i) a certification regarding whether the creation, validation, or substantial modification, including termination, for all existing and proposed covered special access programs, and the compartments and subcompartments within each, are substantiated and justified based on the information required by clause (ii); and

"(ii) for each certification—

"(I) the rationale for the revalidation, validation, or substantial modification, including termination, of each covered special access program, compartment, and subcompartment;

"(II) the identification of a control officer for each covered special access program; and

"(III) a statement of protection requirements for each covered special access program.

"(e) COVERED SPECIAL ACCESS PROGRAM DEFINED.—In this section, the term 'covered special access program' means a special access program that receives funding under the National Intelligence Program or the

Military Intelligence Program, relates to an intelligence or intelligence-related activity, or both.''.

(b) FIRST REPORT.—Not later than 30 days after the date of the enactment of this Act, the head of each element of the intelligence community shall submit to the congressional intelligence committees the first report required under section 501A(d)(1) of the National Security Act of 1947, as added by subsection (a).

(c) CONFORMING REPEAL.—Section 608 of the Intelligence Authorization Act for Fiscal Year 2017 (division N of Public Law 115–31; 131 Stat. 833; 50 U.S.C. 3315) is amended by striking subsection (b).

SEC. 306. CLARIFICATION OF REQUIREMENT FOR AUTHORIZATION OF FUNDING FOR INTELLIGENCE ACTIVITIES.

Paragraph (1) of section 504(a) of the National Security Act of 1947 (50 U.S.C. 3094(a)) is amended to read as follows:

''(1) those funds were specifically authorized by Congress for use for such intelligence or intelligence-related activities; or''.

SEC. 307. AUTHORIZATION OF SUPPORT BY DIRECTOR OF NATIONAL INTELLIGENCE FOR CERTAIN ACTIVITIES RELATING TO INTELLIGENCE COMMUNITY WORKFORCE.

Title X of the National Security Act of 1947 (50 U.S.C. 3191 et seq.) is amended by inserting after section 1024 the following new section (and conforming the table of contents at the beginning of such Act accordingly):

"SEC. 1025. AUTHORIZATION OF SUPPORT BY DIRECTOR OF NATIONAL INTELLIGENCE FOR CERTAIN WORKFORCE ACTIVITIES.

''(a) AUTHORIZATION.—The Director may, with or without reimbursement, obligate or expend amounts authorized to be appropriated or otherwise made available for the Office of the Director of National Intelligence for covered workforce activities for the purpose of supporting a covered workforce activity of an element of the intelligence community.

''(b) COVERED WORKFORCE ACTIVITY DEFINED.—In this section, the term 'covered workforce activity' means an activity relating to—

''(1) recruitment or retention of the intelligence community workforce; or

''(2) diversity, equality, inclusion, or accessibility, with respect to such workforce.''.

SEC. 308. REQUIREMENTS FOR CERTAIN EMPLOYMENT ACTIVITIES BY FORMER INTELLIGENCE OFFICERS AND EMPLOYEES.

(a) MODIFICATIONS TO REQUIREMENT.—

(1) IN GENERAL.—Section 304 of the National Security Act of 1947 (50 U.S.C. 3073a) is amended to read as follows:

"SEC. 304. REQUIREMENTS FOR CERTAIN EMPLOYMENT ACTIVITIES BY FORMER INTELLIGENCE OFFICERS AND EMPLOYEES.

"(a) TEMPORARY RESTRICTION.—An employee of an element of the intelligence community who occupies a covered intelligence position may not occupy a covered post-service position during the 30-month period following the date on which the employee ceases to occupy a covered intelligence position.

"(b) COVERED POST-SERVICE EMPLOYMENT REPORTING.—

"(1) REQUIREMENT.—During the 5-year period beginning on the date on which an employee ceases to occupy a covered intelligence position, the employee shall—

"(A) report covered post-service employment to the head of the element of the intelligence community that employed such employee in such covered intelligence position upon ac-

cepting such covered post-service employment; and

''(B) annually (or more frequently if the head of such element considers it appropriate) report covered post-service employment to the head of such element.

''(2) REGULATIONS.—The head of each element of the intelligence community shall issue regulations requiring, as a condition of employment, each employee of such element occupying a covered intelligence position to sign a written agreement requiring the regular reporting of covered post-service employment to the head of such element pursuant to paragraph (1).

''(c) PENALTIES.—

''(1) CRIMINAL PENALTIES.—A former employee who knowingly and willfully violates subsection (a) or who knowingly and willfully fails to make a required report under subsection (b) shall be fined under title 18, United States Code, or imprisoned for not more than 5 years, or both. Each report under subsection (b) shall be subject to section 1001 of title 18, United States Code.

''(2) SECURITY CLEARANCES.—The head of an element of the intelligence community shall revoke

the security clearance of a former employee if the former employee knowingly and willfully fails to make a required report under subsection (b) or knowingly and willfully makes a false report under such subsection.

''(d) PROVISION OF INFORMATION.—

''(1) TRAINING.—The head of each element of the intelligence community shall regularly provide training on the reporting requirements under subsection (b) to employees of that element who occupy a covered intelligence position.

''(2) WRITTEN NOTICE.—The head of each element of the intelligence community shall provide written notice of the reporting requirements under subsection (b) to an employee when the employee ceases to occupy a covered intelligence position.

''(e) ANNUAL REPORTS.—

''(1) REQUIREMENT.—Not later than March 31 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report on covered post-service employment occurring during the year covered by the report.

''(2) ELEMENTS.—Each report under paragraph (1) shall include the following:

"(A) The number of former employees who occupy a covered post-service position, broken down by—

"(i) the name of the employer;

"(ii) the foreign government, including by the specific foreign individual, agency, or entity, for whom the covered post-service employment is being performed; and

"(iii) the nature of the services provided as part of the covered post-service employment.

"(B) A certification by the Director that—

"(i) each element of the intelligence community maintains adequate systems and processes for ensuring that former employees are submitting reports required under subsection (b);

"(ii) to the knowledge of the heads of the elements of the intelligence community, all former employees who occupy a covered post-service position are in compliance with this section;

"(iii) the services provided by former employees who occupy a covered post-service position do not—

"(I) pose a current or future threat to the national security of the United States; or

"(II) pose a counterintelligence risk; and

"(iv) the Director and the heads of such elements are not aware of any credible information or reporting that any former employee who occupies a covered post-service position has engaged in activities that violate Federal law, infringe upon the privacy rights of United States persons, or constitute abuses of human rights.

"(3) FORM.—Each report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

"(f) NOTIFICATION.—In addition to the annual reports under subsection (e), if a head of an element of the intelligence community determines that the services provided by a former employee who occupies a covered post-service position pose a threat or risk described in clause (iii) of paragraph (2)(B) of such subsection, or include ac-

tivities described in clause (iv) of such paragraph, the head shall notify the congressional intelligence committees of such determination by not later than 7 days after making such determination. The notification shall include the following:

''(1) The name of the former employee.

''(2) The name of the employer.

''(3) The foreign government, including the specific foreign individual, agency, or entity, for whom the covered post-service employment is being performed.

''(4) As applicable, a description of—

''(A) the risk to national security, the counterintelligence risk, or both; and

''(B) the activities that may violate Federal law, infringe upon the privacy rights of United States persons, or constitute abuses of human rights.

''(g) DEFINITIONS.—In this section:

''(1) COVERED INTELLIGENCE POSITION.—The term 'covered intelligence position' means a position within an element of the intelligence community that, based on the level of access of a person occupying such position to information regarding sensitive intelligence sources or methods or other excep-

tionally sensitive matters, the head of such element determines should be subject to the requirements of this section.

''(2) COVERED POST-SERVICE EMPLOYMENT.—The term 'covered post-service employment' means direct or indirect employment by, representation of, or any provision of advice or services relating to national security, intelligence, the military, or internal security to, the government of a foreign country or any company, entity, or other person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized, in whole or in major part, by any government of a foreign country.

''(3) COVERED POST-SERVICE POSITION.—The term 'covered post-service position' means a position of employment described in paragraph (2).

''(4) EMPLOYEE.—The term 'employee', with respect to an employee occupying a covered intelligence position, includes an officer or official of an element of the intelligence community, a contractor of such an element, a detailee to such an element, or a member of the Armed Forces assigned to such an element.

''(5) FORMER EMPLOYEE.—The term 'former employee' means an individual—

"(A) who was an employee occupying a covered intelligence position; and

"(B) who is subject to the requirements under subsection (a) or (b).

"(6) GOVERNMENT OF A FOREIGN COUNTRY.—The term 'government of a foreign country' has the meaning given the term in section 1(e) of the Foreign Agents Registration Act of 1938 (22 U.S.C. 611(e)).".

(2) APPLICATION.—Such section 304, as amended by paragraph (1), shall apply with respect to employees who occupy covered intelligence positions (as defined in such section) on or after the date of the enactment of this Act.

(3) REVISED REGULATIONS.—

(A) SUBMISSION.—Not later than 90 days after the date of the enactment of this Act, the head of each element of the intelligence community shall submit to the congressional intelligence committees new or updated regulations issued under such section 304, as amended by paragraph (1).

(B) CERTIFICATION.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall

submit to the congressional intelligence committees—

(i) a written certification for each head of an element of the intelligence community who has issued the updated regulations under such section 304, as amended by paragraph (1); and

(ii) for each head of an element of the intelligence community who has not issued such updated regulations, an explanation for the failure to issue such updated regulations.

(4) INITIAL REPORT.—In the first report submitted by the Director of National Intelligence under subsection (e) of such section 304, as amended by paragraph (1), the Director shall include an assessment of the licensing requirements under the Arms Export Control Act (22 U.S.C. 2751 et seq.) and recommendations with respect to strengthening the activities regulated under such section 304.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such Act is amended by striking the item relating to section 304 and inserting the following new item:

"Sec. 304. Requirements for certain employment activities by former intelligence officers and employees.".

SEC. 309. NON-REIMBURSABLE DETAIL OF INTELLIGENCE COMMUNITY PERSONNEL TO ASSIST WITH PROCESSING AND RESETTLEMENT OF REFUGEES, PAROLEES, AND OTHER ALIENS FROM AFGHANISTAN.

Section 113A of the National Security Act of 1947 (50 U.S.C. 3049) is amended—

(1) by striking ''An officer'' and inserting ''(a) IN GENERAL.—An officer'';

(2) by striking ''section'' both places it appears and inserting ''subsection''; and

(3) by adding at the end the following new subsection:

''(b) PROCESSING AND RESETTLEMENT OF REFUGEES, PAROLEES, AND OTHER ALIENS FROM AFGHANISTAN.—An officer or employee of an element of the intelligence community may be detailed to another element of the United States Government on a non-reimbursable basis for the purpose of providing assistance with the processing and resettlement of refugees, parolees, and other aliens, from Afghanistan, as jointly agreed to by the heads of the receiving and detailing elements, for a period not to exceed 1 year. This subsection does not limit any other source of authority for reimbursable or non-reimbursable details. A non-reimbursable detail made under this subsection shall not be considered an augmentation of the ap-

propriations of the receiving element of the United States Government.''.

SEC. 310. AUTHORITY FOR TRANSPORT OF CERTAIN CANINES ASSOCIATED WITH FORCE PROTECTION DUTIES OF INTELLIGENCE COMMUNITY.

Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.) is amended by inserting after section 116 the following new section (and conforming the table of contents at the beginning of such Act accordingly):

''SEC. 116A. AUTHORITY FOR TRANSPORTATION OF CERTAIN CANINES ASSOCIATED WITH FORCE PROTECTION DUTIES OF INTELLIGENCE COMMUNITY.

''(a) TRANSPORTATION.—For purposes of section 1344 of title 31, United States Code, the transportation of federally owned canines associated with force protection duties of an element of the intelligence community between the residence of an officer or employee of the element and various locations that is essential for the performance of the force protection duty shall be deemed essential for the safe and efficient performance of intelligence duties.

''(b) OFFICERS AND EMPLOYEES COVERED.—In the administration of section 1344 of title 31, United States Code, an officer or employee of an element of the intel-

ligence community shall be treated as being listed in subsection (b).''.

SEC. 311. DEVELOPMENT OF DEFINITIONS FOR CERTAIN TERMS RELATING TO INTELLIGENCE.

(a) DEVELOPMENT.—Not later than September 30, 2023, the Director of National Intelligence and the Under Secretary of Defense for Intelligence and Security, in consultation with the heads of the elements of the intelligence community, shall jointly develop and publish definitions for the following terms:

(1) Acoustic intelligence.

(2) All-source intelligence.

(3) Communications intelligence.

(4) Critical intelligence.

(5) Cyber-threat intelligence.

(6) Electronic intelligence.

(7) Explosive ordnance intelligence.

(8) General military intelligence.

(9) Imagery intelligence.

(10) Instrumentation signals intelligence.

(11) Intelligence-related activity.

(12) Joint intelligence.

(13) Measurement and signature intelligence.

(14) Medical intelligence.

(15) Open-source intelligence.

(16) Operational intelligence.

(17) Scientific and technical intelligence.

(18) Signals intelligence.

(19) Strategic intelligence.

(20) Tactical intelligence.

(21) Target intelligence.

(22) Technical intelligence.

(23) Such others terms as may be jointly determined necessary by the Director of National Intelligence and the Under Secretary of Defense for Intelligence.

(b) APPLICATION TO ACTIVITIES OF INTELLIGENCE COMMUNITY.—The Director of National Intelligence shall ensure that the definitions developed under subsection (a) are used uniformly across activities of the intelligence community with respect to the corresponding terms specified in such subsection.

(c) NOTICE OF MODIFICATIONS.—The Director of National Intelligence and the Under Secretary of Defense for Intelligence shall submit to the congressional intelligence committees notification of any modification by the Director and Under Secretary to a definition of a term specified in subsection (a) following the initial publication of the definition under such subsection.

(d) DEFINITIONS.—In this section, the terms ''congressional intelligence committees'' and ''intelligence community'' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 312. SUPPORT FOR AND OVERSIGHT OF UNIDENTIFIED AERIAL PHENOMENA TASK FORCE.

(a) AVAILABILITY OF DATA ON UNIDENTIFIED AERIAL PHENOMENA.—The Director of National Intelligence shall ensure that each element of the intelligence community with data relating to unidentified aerial phenomena makes such data available immediately to the Unidentified Aerial Phenomena Task Force, or successor entity, and to the National Air and Space Intelligence Center.

(b) QUARTERLY REPORTS.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, and not less frequently than quarterly thereafter, the Unidentified Aerial Phenomena Task Force, or successor entity, shall submit to the appropriate congressional committees a report on the findings of the Unidentified Aerial Phenomena Task Force, or successor entity.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include, at a minimum, the following:

(A) All reported unidentified aerial phenomena-related events that occurred during the period covered by the report.

(B) All reported unidentified aerial phenomena-related events that occurred during a period other than the period covered by the report but were not included in an earlier report.

(3) FORM.—Each report submitted under paragraph (1) shall be submitted in classified form, consistent with the protection of intelligence sources and methods.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means the following:

(A) The congressional intelligence committees.

(B) The Committees on Armed Services of the House of Representatives and the Senate.

(2) UNIDENTIFIED AERIAL PHENOMENA TASK FORCE.—The term ''Unidentified Aerial Phenomena Task Force'' means the task force established by the Department of Defense on August 4, 2020, to be led by the Department of the Navy, under the Office of

the Under Secretary of Defense for Intelligence and Security.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

SEC. 401. NATIONAL COUNTERPROLIFERATION AND BIOSECURITY CENTER.

(a) REDESIGNATION OF CENTER.—Section 119A of the National Security Act of 1947 (50 U.S.C. 3057) is amended by striking ''National Counter Proliferation Center'' each place it appears and inserting ''National Counterproliferation and Biosecurity Center''.

(b) ESTABLISHMENT AND HEAD.—Subsection (a) of such section is amended—

(1) in paragraph (1)—

(A) by striking ''government tools to prevent'' and inserting ''government tools to—

''(A) prevent'';

(B) by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following new paragraph:

''(2) lead integration and mission management of all intelligence activities pertaining to biosecurity and foreign biological threats.''; and

(2) by adding at the end the following new paragraph:

''(4) The Director of the National Counterproliferation and Biosecurity Center shall serve as the principal coordinator for the intelligence community, and as the principal advisor to the Director of National Intelligence, with respect to biosecurity and foreign biological threats.''.

(c) MISSIONS AND OBJECTIVES.—Subsection (b) of such section is amended—

(1) by redesignating paragraphs (1) through (7) as subparagraphs (A) through (G), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the right;

(2) in the matter preceding subparagraph (A), as so redesignated, by striking ''In establishing'' and inserting the following:

''(1) COUNTERPROLIFERATION.—In establishing''; and

(3) by adding at the end the following new paragraph:

''(2) BIOSECURITY.—In establishing the National Counterproliferation and Biosecurity Center,

the President shall address the following missions and objectives to ensure that the Center serves as the lead for the intelligence community for the integration, mission management, and coordination of intelligence activities pertaining to biosecurity and foreign biological threats, regardless of origin:

''(A) Ensuring that the elements of the intelligence community provide timely and effective warnings to the President and the Director of National Intelligence regarding emerging foreign biological threats, including diseases with pandemic potential.

''(B) Overseeing and coordinating the collection and analysis of intelligence on biosecurity and foreign biological threats in support of the intelligence needs of the Federal departments and agencies responsible for public health, including by conveying collection priorities to elements of the intelligence community.

''(C) Coordinating intelligence support to the Federal departments and agencies responsible for public health, including by ensuring that intelligence pertaining to biosecurity and foreign biological threats is disseminated among

appropriately cleared personnel of such departments and agencies.

''(D) Coordinating with the Federal departments and agencies responsible for public health to encourage information sharing with the intelligence community.

''(E) Identifying gaps in the capabilities of the intelligence community regarding biosecurity and countering foreign biological threats and providing to the Director of National Intelligence recommended solutions for such gaps, including by encouraging research and development of new capabilities to counter foreign biological threats.''.

(d) CONFORMING AMENDMENTS.—Such section is further amended—

(1) by striking ''counter proliferation'' each place it appears and inserting ''counterproliferation''; and

(2) in the section heading, by striking ''COUNTER PROLIFERATION'' and inserting ''COUNTERPROLIFERATION AND BIOSECURITY'' (and conforming the table of sections at the beginning of such Act accordingly).

(e) REFERENCES.—Any reference in any law, regulation, guidance, instruction, or other document of the United States Government to the National Counter Proliferation Center shall be deemed to refer to the National Counterproliferation and Biosecurity Center.

SEC. 402. CLARIFICATION OF CERTAIN RESPONSIBILITY OF THE DIRECTOR OF NATIONAL INTELLIGENCE.

Section 102A(f)(8) of the National Security Act of 1947 (50 U.S.C. 3024(f)(8)) is amended by striking ''such other functions'' and inserting ''such other intelligence-related functions''.

SEC. 403. RESPONSIBILITY OF DIRECTOR OF NATIONAL INTELLIGENCE REGARDING NATIONAL INTELLIGENCE PROGRAM BUDGET CONCERNING FEDERAL BUREAU OF INVESTIGATION.

Section 102A of the National Security Act of 1947 (50 U.S.C. 3024) is amended by adding at the end the following new subsection:

''(aa) RESPONSIBILITY OF DIRECTOR OF NATIONAL INTELLIGENCE REGARDING NATIONAL INTELLIGENCE PROGRAM BUDGET CONCERNING FEDERAL BUREAU OF INVESTIGATION.—(1) Consistent with subsection (c)(5)(C), the Director of National Intelligence shall, after consultation with the Director of the Federal Bureau of

Investigation, ensure that the programs and activities of the Federal Bureau of Investigation that are part of the National Intelligence Program are executed in a manner that conforms with the requirements of the national intelligence strategy under section 108A and the National Intelligence Priorities Framework of the Office of the Director of National Intelligence (or any successor mechanism established for the prioritization of such programs and activities).

''(2) Consistent with subsection (c)(5)(C), the Director of National Intelligence shall ensure that the programs and activities that are part of the National Intelligence Program, including those of the Federal Bureau of Investigation, are structured and executed in a manner than enables budget traceability.''.

SEC. 404. CLIMATE SECURITY ADVISORY COUNCIL.

(a) REPORTS.—Subsection (d) of section 120 of the National Security Act of 1947 (50 U.S.C. 3060) is amended—

(1) by striking ''Not later'' and inserting the following:

''(1) REQUIREMENT.—Not later''; and

(2) by adding at the end the following new paragraph:

''(2) MATTERS INCLUDED.—Each report under paragraph (1) shall include a description of any obstacles or gaps relating to—

''(A) the Council fulfilling its duties and responsibilities under subsection (c); or

''(B) the responsiveness of the intelligence community to the climate security needs and priorities of the policymaking elements of the Federal Government.''.

(b) EXTENSION OF SUNSET; TECHNICAL AMENDMENTS.—Such section 120 is amended—

(1) in subsection (b)(1)(B)(v), by inserting ''and Security'' after ''for Intelligence'';

(2) by redesignating the second subsection (e) as subsection (f); and

(3) in subsection (e), by striking ''the date that is 4 years after the date of the enactment of this section'' and inserting ''December 31, 2025''.

Subtitle B—Other Elements

SEC. 411. PROTECTION OF CERTAIN FACILITIES AND ASSETS OF CENTRAL INTELLIGENCE AGENCY FROM UNMANNED AIRCRAFT.

The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.) is amended by inserting after section 15 the following new section:

"SEC. 15A. PROTECTION OF CERTAIN FACILITIES AND ASSETS OF CENTRAL INTELLIGENCE AGENCY FROM UNMANNED AIRCRAFT.

"(a) AUTHORITY.—In accordance with subsection (b), the Director shall have the same authority for the Agency as is available to the Secretary of Homeland Security for the Department of Homeland Security and the Attorney General for the Department of Justice under section 210G of the Homeland Security Act of 2002 (6 U.S.C. 124n), and shall be subject to the same limitations and requirements under such section.

"(b) ADMINISTRATION.—For purposes of subsection (a)—

"(1) the reference in subsection (i) of section 210G of the Homeland Security Act of 2002 (6 U.S.C. 124n) to 'the date that is 4 years after the date of enactment of this section' shall be deemed to be a reference to 'October 5, 2026';

"(2) the term 'appropriate congressional committees' as defined in paragraph (1) of subsection (k) of such section shall be deemed to mean the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate; and

"(3) the term 'covered facility or asset' as defined in paragraph (3) of such subsection (k) shall

be deemed to mean installations, property, and persons—

"(A) that are located in the United States;

"(B) for which the Director may provide protection pursuant to section 5(a)(4) or 15(a)(1) of this Act; and

"(C) that the Director identifies as high-risk and a potential target for unlawful unmanned aircraft activity.".

SEC. 412. MODIFICATION OF NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY PERSONNEL MANAGEMENT AUTHORITY TO ATTRACT EXPERTS IN SCIENCE AND ENGINEERING.

Section 1599h(b)(2)(A) of title 10, United States Code, is amended—

(1) by striking "paragraph (1)(B)" and inserting "subparagraph (B) of paragraph (1)"; and

(2) by inserting "or employees appointed pursuant to the first subparagraph (G) of such paragraph to any of 2 positions of administration or management designated by the Director of the National Geospatial-Intelligence Agency for purposes of this subparagraph" after "this subparagraph".

SEC. 413. REQUIREMENTS FOR TERMINATION OF DUAL-HAT ARRANGEMENT FOR COMMANDER OF THE UNITED STATES CYBER COMMAND.

Section 1642 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 130 Stat. 2601), as amended by section 1636 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1748), is further amended—

(1) by striking subsections (a), (b), and (c), and inserting the following new subsections:

''(a) LIMITATION ON TERMINATION OF DUAL-HAT ARRANGEMENT.—The Secretary of Defense may not terminate the dual-hat arrangement until the date on which the Secretary submits to the appropriate committees of Congress the certification under subsection (b)(1). The Secretary shall implement such termination by not later than the first day of the fiscal year following the fiscal year in which the Secretary submits such certification.

''(b) ANNUAL SUBMISSION OF INFORMATION.—Together with the defense budget materials for fiscal year 2023, and annually thereafter until the termination of the dual-hat arrangement, the Secretary of Defense, in coordination with the Director of National Intelligence, shall submit to the appropriate committees of Congress a report containing either of the following:

"(1) A certification that the United States Cyber Command has met each of the following conditions:

"(A) Sufficient operational infrastructure has been deployed to meet the unique cyber mission needs of the United States Cyber Command.

"(B) Sufficient command and control systems and processes have been established for planning, deconflicting, and executing military cyber operations.

"(C) Capabilities have been established to enable intelligence collection and operational preparation of the environment for cyber operations consistent with the United States Cyber Command reaching full operational status.

"(D) Mechanisms have been established to train cyber operations personnel, test cyber capabilities, and rehearse cyber missions.

"(E) The United States Cyber Command has achieved full operational capability.

"(2) If the Secretary, in coordination with the Director, is not able to make the certification under paragraph (1)—

"(A) an identification of the items contained in the defense budget materials that are related to meeting the conditions specified in such paragraph; and

"(B) an assessment of the funding required to meet such conditions during the period covered by the future-years defense program under section 221 of title 10, United States Code.";

(2) by redesignating subsection (d) as subsection (c); and

(3) in subsection (c), as so redesignated, by adding at the end the following new paragraph:

"(3) DEFENSE BUDGET MATERIALS.—The term 'defense budget materials' has the meaning given that term in section 231(f) of title 10, United States Code.".

SEC. 414. NATIONAL SPACE INTELLIGENCE CENTER.

(a) FINDINGS.—Congress finds the following:

(1) Section 9081 of title 10, United States Code, establishes the United States Space Force as an Armed Force within the Department of the Air Force to, as stated in subsection (c) of such section—

(A) provide freedom of operation for the United States in, from, and to space;

(B) conduct space operations; and

(C) protect the interests of the United States in space.

(2) The National Air and Space Intelligence Center, headquartered at Wright-Patterson Air Force Base, Ohio, is the primary source for foreign air and space threat analysis within the intelligence enterprise of the Air Force.

(3) Section 8041 of the Department of Defense Appropriations Act, 2020 (division A of Public Law 116–93; 133 Stat. 2345) prohibits the establishment of a new field operating agency using funds made available under that Act, although the Secretary of Defense or the Secretary of a military department may waive the prohibition in cases where the relevant Secretary determines that the establishment will reduce the personnel or financial requirements of the relevant department.

(b) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) space has become increasingly contested, congested, and competitive, mandating an expanded need for space intelligence;

(2) to support this increasingly complex operational environment, the Space Force should have its own intelligence organization dedicated to providing the Joint Combat forces with the required intelligence and analysis to support operations;

(3) a prominent factor in the basing decision should consider that co-locating the National Space Intelligence Center with the National Air and Space Intelligence Center at Wright-Patterson Air Force Base will provide an operational and geographic synergy which will greatly benefit combat operations across the air and space operational environments;

(4) the Air Force has requested authority to establish the National Space Intelligence Center as a field operating agency to ensure the appropriate prioritization of analytic effort for the space domain, enhance responsiveness to national-level customers, and align command relationships with the Director of Intelligence, Surveillance, and Reconnaissance of the Space Force; and

(5) establishing the National Space Intelligence Center as a field operating agency would be a resource-neutral administrative realignment of billets, and would facilitate a lean and agile space intelligence enterprise.

(c) EXCEPTION.—Notwithstanding section 8041 of the Department of Defense Appropriations Act, 2020 (division A of Public Law 116–93; 133 Stat. 2345), or any other provision of law prohibiting the establishment of a field operating agency, the Secretary of the Air Force may establish the National Space Intelligence Center as a field operating agency of the Space Force to perform the analysis and production of scientific and technical intelligence on foreign space and counter-space threat capabilities in the support of the Space Force.

SEC. 415. PROCUREMENT BY FEDERAL BUREAU OF INVESTIGATION OF CHINESE PRODUCTS AND SERVICES.

(a) SECURITY ASSESSMENT.—The Director of the Federal Bureau of Investigation may not procure a Chinese product or service unless, before such procurement, the Counterintelligence Division of the Federal Bureau of Investigation—

(1) conducts a security assessment of such product or service, including with respect to any physical or cyber vulnerabilities; and

(2) makes a recommendation to the Director regarding such proposed procurement.

(b) SUBMISSION.—Not later than 30 days after the date on which the Counterintelligence Division of the Bu-

reau conducts a security assessment under subsection (a), the Director shall submit to the congressional intelligence committees a copy of such assessment and the recommendation under paragraph (2) of such subsection.

(c) CHINESE PRODUCT OR SERVICE DEFINED.—In this section, the term ''Chinese product or service'' means a product or service provided by an entity that is owned or controlled by, or otherwise connected to, the government of China.

SEC. 416. COUNTERINTELLIGENCE UNITS AT NON-INTELLIGENCE COMMUNITY FEDERAL DEPARTMENTS AND AGENCIES.

(a) ESTABLISHMENT.—The Director of the Federal Bureau of Investigation shall establish counterintelligence units in the departments and agencies described in subsection (b). Such units shall be composed of officers of the Counterintelligence Division of the Federal Bureau of Investigation.

(b) DEPARTMENTS AND AGENCIES DESCRIBED.—The departments and agencies described in this subsection are the following departments and agencies of the United States Government:

(1) The Department of Agriculture.

(2) Any other department or agency that the Director, in coordination with the Director of National Intelligence, determines appropriate.

(c) DUTIES.—The Director of the Federal Bureau of Investigation shall ensure that each counterintelligence unit established under subsection (a) in a department or agency described in subsection (b) carries out the following duties:

(1) Conducts assessments, in coordination with the leadership of the department or agency, to determine the counterintelligence posture of the department or agency, including any components thereof.

(2) Informs and consults with the leadership of the department or agency, including any components thereof, and provides recommendations with respect to any counterintelligence threats identified by the intelligence community.

(3) Provides such administrative and technical support as is necessary to develop, in coordination with the leadership of the department or agency, a plan to eliminate or reduce the threats described in paragraph (2).

(4) Serves as the primary point of contact for the department or agency with respect to counterintelligence for the intelligence community.

(d) INTELLIGENCE COMMUNITY SUPPORT.—The heads of the elements of the intelligence community shall ensure that relevant counterintelligence information is provided to counterintelligence units established under subsection (a) in a manner that is consistent with the need to protect sources and methods.

SEC. 417. DETECTION AND MONITORING OF WILDFIRES.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the Director of the National Geospatial-Intelligence Agency, in accordance with relevant provisions of law, should continue to manage the systems of the National Geospatial-Intelligence Agency that enable the FireGuard program of the Department of Defense.

(b) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Director of the National Geospatial-Intelligence Agency, in consultation with the Secretary of Defense and the heads of the departments and agencies of the United States Government and other organizations that constitute the National Interagency Fire Center, and any other relevant organization the Director determines appropriate, shall submit to the appropriate congressional committees a coordinated interagency report that—

(1) explains how to leverage existing resources to improve processes and organization alignment;

(2) identifies future opportunities to improve the ability to detect and track wildfires and support firefighting efforts; and

(3) includes an explication of the relevant authorities with respect to the matters under paragraphs (1) and (2).

(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the congressional intelligence committees; and

(2) the congressional defense committees (as defined in section 101(a)(16) of title 10, United States Code).

TITLE V—ANOMALOUS HEALTH INCIDENTS AND OTHER HEALTH CARE MATTERS

SEC. 501. COMPENSATION AND PROFESSIONAL STANDARDS FOR CERTAIN MEDICAL OFFICERS OF THE CENTRAL INTELLIGENCE AGENCY.

The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.) is amended by adding at the end the following new section:

"SEC. 26. COMPENSATION AND PROFESSIONAL STANDARDS FOR CERTAIN MEDICAL OFFICERS.

"(a) OFFICE OF MEDICAL SERVICES.—There is in the Agency an Office of Medical Services.

"(b) COMPENSATION.—Beginning not later than 1 year after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, each medical officer of the Office of Medical Services who meets the qualifications under subsection (c) shall be compensated during a pay period pursuant to a pay range that is equal to the pay range published in the Federal Register pursuant to section 7431(e)(1)(C) of title 38, United States Code (for the corresponding pay period), for a physician in the Veterans Health Administration in the District of Columbia region with a medical subspecialty that is the equivalent of the medical subspecialty of the officer.

"(c) CLINICAL PRACTICE QUALIFICATIONS.—A medical officer meets the qualifications under this subsection if the officer provides direct care services to patients in connection with the official duties of the officer and—

"(1) maintains current, active, full, and unrestricted licensure or registration as a physician from a State, the District of Columbia, or a commonwealth or territory of the United States;

"(2) holds active board certification and maintains accreditation in an American Board of Medical Specialties direct care clinical specialty; and

"(3) except as provided in subsection (d), maintains a minimum of 160 hours per year of clinical practice in an accredited clinic or hospital facility that is not affiliated with the Central Intelligence Agency.

"(d) EXCEPTION FOR OVERSEAS SERVICE.—If a medical officer is a medical officer located in a duty station outside of the United States pursuant to a permanent change of station and greater than 50 percent of the official duties of the officer in such duty station involve direct patient care, the officer, in lieu of performing the minimum hours under subsection (c)(3) on an annual basis, may perform up to 480 hours of clinical practice as specified in such subsection prior to such change of station, to fulfil in advance the requirement under such subsection for up to 3 years.

"(e) CLINICAL PRACTICE HOURS.—The head of the Office of Medical Services shall make available to medical officers excused absence time to allow for the maintenance of clinical practice hours in accordance with subsection (c)(3).".

SEC. 502. MEDICAL ADVISORY BOARD OF THE CENTRAL INTELLIGENCE AGENCY.

(a) ESTABLISHMENT.—The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.), as amended by section 501, is further amended by adding at the end the following new section:

"SEC. 27. MEDICAL ADVISORY BOARD.

"(a) ESTABLISHMENT.—The Director shall establish within the Agency a medical advisory board (in this section referred to as the 'Board').

"(b) DUTIES.—The Board shall—

"(1) conduct a study on the Office of Medical Services of the Agency, and submit reports regarding such study, in accordance with subsection (c); and

"(2) upon request, provide advice and guidance in connection with any independent review of the Office conducted by an inspector general.

"(c) STUDY.—

"(1) OBJECTIVES.—In conducting the study under subsection (b)(1), the Board shall seek to—

"(A) contribute to the modernization and reform of the Office of Medical Services;

"(B) ensure that the activities of the Office are of the highest professional quality; and

"(C) ensure that all medical care provided by the Office is provided in accordance with the highest professional medical standards.

"(2) REPORTS.—The Board shall submit to the congressional intelligence committees, in writing—

"(A) interim reports on the study; and

"(B) a final report on the study, which shall—

"(i) set forth in detail the findings of the study and the recommendations of the Board, based on such findings and taking into consideration the objectives under paragraph (1), regarding any changes to the activities of the Office of Medical Services; and

"(ii) include, as applicable, any additional or dissenting views submitted by a member of the Board.

"(d) MEMBERSHIP.—

"(1) NUMBER AND APPOINTMENT.—The Board shall be composed of 11 members, appointed as follows:

"(A) 2 members appointed by the Chairman of the Permanent Select Committee on Intelligence of the House of Representatives.

"(B) 2 members appointed by the ranking minority member of the Permanent Select Committee on Intelligence of the House of Representatives.

"(C) 2 members appointed by the Chairman of the Select Committee on Intelligence of the Senate.

"(D) 2 members appointed by the Vice Chairman of the Select Committee on Intelligence of the Senate.

"(E) 3 members appointed by the Director of National Intelligence.

"(2) CHAIRPERSON.—During the first meeting under subsection (e)(1), the members of the Board shall elect a Chairperson of the Board. In addition to meeting the criteria under paragraph (3), the Chairperson may not be an employee, or former employee, of the Agency.

"(3) CRITERIA.—The members appointed under paragraph (1) shall meet the following criteria:

"(A) Each member shall be a recognized expert in at least 1 medical field, as demonstrated by appropriate credentials.

"(B) Each member shall possess significant and diverse medical experience, including clinical experience.

"(C) Each member shall hold a security clearance at the top secret level and be able to access sensitive compartmented information.

"(4) TERMS.—

"(A) IN GENERAL.—Each member, including the Chairperson, shall be appointed or elected, as applicable, for the life of the Board.

"(B) VACANCIES.—Any vacancy in the Board occurring prior to the expiration of the term under subparagraph (A) shall be filled in the manner in which the original appointment or election was made.

"(5) COMPENSATION AND TRAVEL EXPENSES.—

"(A) COMPENSATION.—Except as provided in subparagraph (B), each member of the Board, including the Chairperson, may be compensated at not to exceed the daily equivalent of the annual rate of basic pay in effect for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member

is engaged in the actual performance of the duties under subsection (b).

"(B) EXCEPTION FOR FEDERAL EMPLOYEES.—Members of the Board, including the Chairperson, who are officers or employees of the United States shall receive no additional pay by reason of the service of the member on the Board.

"(C) TRAVEL EXPENSES.—Each member of the Board, including the Chairperson, while away from the home or regular places of business of the member in the performance of services for the Board, may be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703 of title 5, United States Code.

"(6) DETAILEES.—

"(A) IN GENERAL.—Upon request of the Board, the Director of National Intelligence may detail to the Board, without reimbursement from the Board, any of the personnel of the Office of the Director of National Intelligence to assist in carrying out the duties

under subsection (b). Any such detailed personnel shall retain the rights, status, and privileges of the regular employment of the personnel without interruption.

''(B) CLEARANCE.—Any personnel detailed to the Board under subparagraph (A) shall possess a security clearance in accordance with applicable laws and regulations concerning the handling of classified information.

''(e) MEETINGS.—

''(1) BOARD MEETINGS.—The Board shall meet not less frequently than on a quarterly basis.

''(2) MEETINGS WITH CONGRESS.—The Board shall meet with the congressional intelligence committees on a biannual basis.

''(f) INFORMATION ACCESS.—

''(1) IN GENERAL.—Except as provided in paragraph (2), the Board may secure directly from any department or agency of the United States Government information necessary to enable it to carry out the duties under subsection (b) and, upon request of the Chairperson of the Board, the head of that department or agency shall furnish such information to the Board.

"(2) EXCEPTION.—The Director (without delegation) may deny a request for information made by the Board pursuant to paragraph (1), regardless of the agency from which such information is requested.

"(3) NOTIFICATION REQUIREMENT.—If the Director denies a request under paragraph (2), not later than 15 days after the date of such denial, the Director shall submit to the congressional intelligence committees a written notification of such denial.

"(4) BRIEFINGS.—The Director shall ensure that the Board receives comprehensive briefings on all activities of the Office, including by promptly scheduling such briefings at the request of the Board.

"(g) TERMINATION.—The Board shall terminate on the date that is 5 years after the date of the first meeting of the Board.

"(h) DEFINITIONS.—In this section, the terms 'congressional intelligence committees' and 'intelligence community' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).".

(b) DEADLINE FOR APPOINTMENTS; FIRST MEETINGS.—

(1) DEADLINE FOR APPOINTMENTS.—Each member of the medical advisory board established under section 27 of the Central Intelligence Agency Act of 1949 (as added by subsection (a)), including the Chairperson, shall be appointed or elected, as applicable, in accordance with subsection (d) of such section by not later than 45 days after the date of the enactment of this Act.

(2) FIRST BOARD MEETING.—Not later than 30 days after the first date on which at least 7 members of the Board described in paragraph (1) hold the security clearance and are able to access information in accordance with subsection (d)(3)(C) of such section 27, the Board shall meet. During such meeting, the Director of the Central Intelligence Agency shall provide to the Board a comprehensive briefing on all aspects of the Office of Medical Services of the Central Intelligence Agency.

(3) FIRST MEETING WITH CONGRESS.—Not later than 30 days after the date of the briefing under paragraph (2), the Board described in such paragraph shall meet with the staff members of the congressional intelligence committees to discuss top-

ics for the Board to examine in carrying out the duties under subsection (b) of such section 27.

SEC. 503. REPORT ON PROTOCOLS FOR CERTAIN INTELLIGENCE COMMUNITY EMPLOYEES AND DEPENDENTS.

(a) IN GENERAL.—Beginning not later than 180 days after the date of enactment of this Act, the President shall develop, for uniform implementation across the elements of the intelligence community, each of the protocols described in subsections (c) through (f). Such protocols shall be subject to review and revision on a periodic basis, and any implementation of such protocols shall be conducted in accordance with applicable laws and current clinical and professional practices of the interagency medical community.

(b) PRIVACY.—No data collected pursuant to any protocol under this section may be used for research or analytical purposes without the written consent of the individual from whom such data was collected with respect to such use.

(c) PROTOCOL ON BASELINE MEDICAL TESTING.—The protocol described in this subsection is a protocol for conducting baseline medical testing of covered employees, covered individuals, and the dependents of covered employees who are included on the overseas travel orders of the

covered employee, with respect to anomalous health incidents. Such protocol shall set forth the required elements of such baseline medical testing, such as—

(1) standard lab collection and testing of relevant biofluids;

(2) the conduct of relevant visual and auditory examinations;

(3) the conduct of Acquired Brain Injury Tool assessments, or other relevant assessments for balance, eye motion, and cognition;

(4) the assessment of relevant medical histories; and

(5) the conduct of any other standard relevant medical or neurological examinations, testing, or assessments.

(d) PROTOCOLS ON POST-INCIDENT MEDICAL TESTING.—The protocols described in this subsection are protocols to enable voluntary medical testing and the coordination of treatment for covered employees, covered individuals, and the dependents of covered employees, following a reported anomalous health incident, such as—

(1) a protocol that sets forth elements, similar to the elements described in subsection (c), of such testing;

(2) a protocol pertaining to the voluntary testing and treatment for victims of anomalous health incidents who are children;

(3) a protocol for ensuring that all victims of anomalous health incidents receive access to prompt and consistent medical treatment, including from medical professionals holding appropriate security clearances and medical professionals with expertise in child care;

(4) a protocol for ensuring that all victims of anomalous health incidents are offered options for psychological treatment for the effects of such incidents; and

(5) a protocol for ensuring that any testing, evaluation, or collection of biofluids or other samples following a reported anomalous health incident may be compared against the baseline for the victim of the anomalous health incident, to the extent the individual participated in the baseline medical testing, consistent with subsections (b) and (c).

(e) PROTOCOL ON INFORMATION COLLECTION, STORAGE, AND SAFEGUARDING.—The protocol described in this subsection is a protocol for the collection, storage, and safeguarding of information acquired as a result of the protocols described in subsections (c) and (d).

(f) PROTOCOL ON REPORTING MECHANISMS.—The protocol described in this subsection is a protocol for the reporting of matters relating to anomalous health incidents by covered employees, covered individuals, and the dependents of covered employees, including the development of a system for the adjudication of complaints regarding medical treatment received by such covered employees, covered individuals, and dependents of covered employees.

(g) REPORT AND BRIEFINGS.—

(1) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the protocols described in subsections (c) through (f).

(2) ELEMENTS.—Such report shall include the following elements:

(A) A copy of each protocol under this section.

(B) A description of the following:

(i) Any interagency agreements, authorities, or policies required to effectively implement the protocols under this section.

(ii) Any new facilities, medical equipment, tools, training, or other resources re-

quired to effectively implement such protocols.

(C) A timeline for the implementation of the protocols under this section, including a proposal for the prioritization of implementation with respect to various categories of covered employees and the dependents of covered employees.

(3) BRIEFING.—Not later than 60 days following the date of submission of the report under paragraph (1), and biannually thereafter, the Director shall provide to the congressional intelligence committees a briefing regarding the implementation of the protocols under this section.

(h) DEFINITIONS.—In this section:

(1) COVERED EMPLOYEE.—The term ''covered employee'' means an individual who is an employee, assignee, or detailee of an element of the intelligence community.

(2) COVERED INDIVIDUAL.—The term ''covered individual'' means a contractor to an element of the intelligence community.

(3) DEPENDENT OF A COVERED EMPLOYEE.—The term ''dependent of a covered employee'' means, with respect to a covered employee, a family member

(including a child), as defined by the Director of National Intelligence.

(4) VICTIM OF AN ANOMALOUS HEALTH INCIDENT.—The term ''victim of an anomalous health incident'' means a covered employee, covered individual, or dependent of a covered employee, who is, or is suspected to have been, affected by an anomalous health incident.

SEC. 504. INSPECTOR GENERAL OF THE CENTRAL INTELLIGENCE AGENCY REVIEW OF OFFICE OF MEDICAL SERVICES.

(a) REVIEW.—Not later than one year after the date of the enactment of this Act, the Inspector General of the Central Intelligence Agency, in coordination with, and with the support of, the Inspector General of the Intelligence Community, shall submit to the congressional intelligence committees a report containing a review of the responsibilities, authorities, resources, and performance of the Office of Medical Services of the Central Intelligence Agency (in this section referred to as the ''Office'').

(b) MATTERS INCLUDED.—The review under subsection (a) shall include the following:

(1) A detailed description of the responsibilities and authorities of the Office, as set forth in Federal

law and any applicable regulation, policy, or other document of the Central Intelligence Agency.

(2) A detailed description of the budgetary, human, and other resources available to the Office, including with respect to employees and any other personnel.

(3) An assessment of the ability of the Office to consistently discharge the responsibilities of the Office, with an emphasis on the provision of medical treatment and care by personnel of the Office, including with respect to—

(A) the roles of personnel of the Office, and of senior officials of the Agency outside of the Office, in determining what medical evaluation, treatment, and care should be provided in a particular case, including the provision of specialty care by medical personnel outside of the Office;

(B) whether personnel of the Office consistently provide appropriate and high-quality medical treatment and care in accordance with standards set independently by the professional medical community;

(C) whether the Office has sufficient human and other resources, including personnel

with specialized background, qualifications, or expertise, to consistently provide high-quality medical treatment and care in accordance with standards set independently by the professional medical community;

(D) whether personnel of the Office, including personnel claiming specialized medical backgrounds and expertise, are required by the Agency to maintain current board certifications or other certifications and licenses, and the extent to which the Office verifies such certifications and licenses;

(E) the extent to which the Office makes consistent and effective use of the specialized medical background, qualifications, and expertise of the personnel of the Office in providing medical treatment and care;

(F) an assessment of whether personnel of the Office who provide medical treatment and care, or who make decisions with respect to such treatment or care, are required to have extensive clinical or other experience in directly treating patients, including in areas requiring specialized background, qualifications, or expertise;

(G) any factors that have frustrated or delayed the provision of medical treatment and care by personnel of the Office in significant cases; and

(H) any factors that have frustrated or could frustrate prompt detection, effective oversight, and swift remediation of problems within the Office, including such factors that frustrate or delay the provision of medical treatment and care in significant cases.

(c) INDEPENDENT ADVICE.—In conducting the review under subsection (a), the Inspector General may obtain the advice of the medical advisory board established under section 502.

(d) FORM.—The report under subsection (a) shall be submitted in an unclassified form to the extent practicable, consistent with the protection of intelligence sources and methods, but may include a classified annex.

SEC. 505. CLARIFICATION OF EFFECT OF CERTAIN BENEFITS RELATING TO INJURIES TO THE BRAIN.

(a) PERSONNEL OF CENTRAL INTELLIGENCE AGENCY.—Subsection (d) of section 19A of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3519b), as added by the HAVANA Act of 2021, is amended by adding at the end the following new paragraph:

"(5) NO EFFECT ON OTHER BENEFITS.—Payments made under paragraph (2) are supplemental to any other benefit furnished by the United States Government for which a covered dependent, covered employee, or covered individual is entitled, and the receipt of such payments may not affect the eligibility of such a person to any other benefit furnished by the United States Government.".

(b) PERSONNEL OF DEPARTMENT OF STATE.—Subsection (i) of section 901 of title IX of division J of the Further Consolidated Appropriations Act, 2020 (22 U.S.C. 2680b), as added by the HAVANA Act of 2021, is amended by adding at the end the following new paragraph:

"(5) NO EFFECT ON OTHER BENEFITS.—Payments made under paragraph (2) are supplemental to any other benefit furnished by the United States Government for which a covered dependent, dependent of a former employee, covered employee, former employee, or covered individual is entitled, and the receipt of such payments may not affect the eligibility of such a person to any other benefit furnished by the United States Government.".

TITLE VI—MATTERS RELATING TO FOREIGN COUNTRIES

SEC. 601. NATIONAL INTELLIGENCE ESTIMATE ON SECURITY SITUATION IN AFGHANISTAN AND RELATED REGION.

(a) REQUIREMENT.—The Director of National Intelligence, acting through the National Intelligence Council, shall produce a National Intelligence Estimate on the situation in Afghanistan and the covered region.

(b) MATTERS.—The National Intelligence Estimate produced under subsection (a) shall include, with respect to the 2-year period beginning on the date on which the Estimate is produced, an assessment of the following:

(1) The presence in Afghanistan (including financial contributions to the Taliban, political relations with the Taliban, military presence in the covered region, economic presence in the covered region, and diplomatic presence in the covered region) of China, Iran, Pakistan, Russia, and any other foreign country determined relevant by the Director, respectively, and an assessment of the potential risks, or benefits, of any such presence, contributions, or relations.

(2) Any change in the threat to the United States homeland or United States entities abroad as

a result of the withdrawal of the Armed Forces from Afghanistan on August 31, 2021, including an assessment of the risk of al-Qaeda or any affiliates thereof, the Islamic State of Iraq and ash Sham-Khorasan or any affiliates thereof, or any other similar international terrorist group, using Afghanistan as a safe haven for launching attacks on the United States and its interests abroad.

(3) The political composition and sustainability of the governing body of Afghanistan, including an assessment of the ability of the United States Government to influence the policies of such governing body on the following:

(A) Counterterrorism.

(B) Counternarcotics.

(C) Human rights (particularly regarding women and girls and traditionally targeted ethnic groups).

(D) The treatment and safe transit of Afghans holding special immigrant visa status under section 602 of the Afghan Allies Protection Act of 2009 (8 U.S.C. 1101 note) and other Afghans who, during the period beginning in 2001, assisted efforts of the United States in Afghanistan or the covered region.

(4) The effect on the covered region, and Europe, of refugees leaving Afghanistan.

(5) The commitments of the Taliban relating to counterterrorism, including an assessment of—

(A) whether such commitments required under the agreement entered into between the United States Government and the Taliban in February 2020, have been tested, or will be tested during the 2-year period covered by the Estimate, and what such commitments entail;

(B) whether any additional commitments relating to counterterrorism agreed to by the Taliban pursuant to subsequent negotiations with the United States Government following February 2020, have been tested, or will be tested during the 2-year period covered by the Estimate, and, if applicable, what such commitments entail;

(C) any benchmarks against which the Taliban are to be evaluated with respect to commitments relating to counterterrorism; and

(D) the intentions and capabilities of the Taliban with respect to counterterrorism (as such term is understood by the United States and by the Taliban, respectively), including the

relations of the Taliban with al-Qaeda or any affiliates thereof, the Islamic State of Iraq and ash Sham-Khorasan or any affiliates thereof, or any other similar international terrorist group.

(c) SUBMISSION TO CONGRESS.—

(1) SUBMISSION.—Not later than one year after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees the National Intelligence Estimate produced under subsection (a), including all intelligence reporting underlying the Estimate.

(2) FORM.—The National Intelligence Estimate shall be submitted under paragraph (1) in classified form.

(d) PUBLIC VERSION.—Consistent with the protection of intelligence sources and methods, at the same time as the Director submits to the congressional intelligence committees the National Intelligence Estimate under subsection (c), the Director shall make publicly available on the internet website of the Director an unclassified version of the key findings of the National Intelligence Estimate.

(e) DEFINITIONS.—In this section:

(1) COVERED REGION.—The term ''covered region'' includes the following countries:

(A) China.

(B) The Gulf Cooperation Council countries, including Qatar, Saudi Arabia, the United Arab Emirates.

(C) India.

(D) Iran.

(E) Pakistan.

(F) Tajikistan.

(G) Turkey.

(H) Turkmenistan.

(I) Uzbekistan.

(2) UNITED STATES ENTITY.—The term ''United States entity'' means a citizen of the United States, an embassy or consulate of the United States, or an installation, facility, or personnel of the United States Government.

SEC. 602. REPORT ON LIKELIHOOD OF MILITARY ACTION BY COUNTRIES OF THE SOUTH CAUCASUS.

(a) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report assessing the likelihood of a South Caucasus country taking military action against another country (including in Nagorno-Karabakh or any other disputed territory). Such report shall include an indication of the strategic balance in the region, including with re-

spect to the offensive military capabilities of each South Caucasus country.

(b) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(c) SOUTH CAUCASUS COUNTRY DEFINED.—In this section, the term ''South Caucasus country'' means any of the following:

(1) Armenia.

(2) Azerbaijan.

(3) Georgia.

SEC. 603. REPORT ON INTELLIGENCE COLLECTION POSTURE AND OTHER MATTERS RELATING TO AFGHANISTAN AND RELATED REGION.

(a) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of elements of the intelligence community determined relevant by the Director, shall submit to the congressional intelligence committees a report on the collection posture of the intelligence community and other matters relating to Afghanistan and the covered region.

(b) MATTERS.—The report under subsection (a) shall include the following:

(1) A detailed description of the collection posture of the intelligence community with respect to Afghanistan, including with respect to the following:

(A) The countering of terrorism threats that are directed at the United States homeland or United States entities abroad.

(B) The finances of the Taliban, including financial contributions to the Taliban from foreign countries (particularly from China, Iran, Russia, and any other foreign country in the Arab Gulf region (or elsewhere) determined relevant by the Director, respectively).

(C) The detection, and prevention of, any increased threat to the United States homeland or United States entities abroad as a result of the withdrawal of the United States Armed Forces from Afghanistan on August 31, 2021, including any such increased threat resulting from al-Qaeda or any affiliates thereof, the Islamic State of Iraq and ash Sham-Khorasan or any affiliates thereof, or any other similar international terrorist group, using Afghanistan as a safe harbor.

(2) A detailed description of any plans, strategies, or efforts to improve the collection posture de-

scribed in paragraph (1)(A), including by filling any gaps identified pursuant to such paragraph.

(3) An assessment of the effect of publicly documenting abuses engaged in by the Taliban, and a description of the efforts of the intelligence community to support other departments and agencies in the Federal Government with respect to the collection and documentation of such abuses.

(4) An assessment of the relationship between the intelligence community and countries in the covered region, including an assessment of the following:

(A) Intelligence and information sharing with such countries.

(B) Any change in the collection posture of the intelligence community with respect to the nuclear activities of such countries as a result of the withdrawal of the United States Armed Forces from Afghanistan on August 31, 2021.

(C) The collection posture of the intelligence community with respect to the presence of such countries in Afghanistan (including financial contributions to the Taliban, political relations with the Taliban, military presence in Afghanistan, economic presence in Afghanistan,

and diplomatic presence in Afghanistan) and the understanding of the intelligence community regarding the potential risks, or benefits, of any such presence, contributions, or relations.

(D) The ability of the intelligence community to use the airspace of any such countries.

(5) An assessment of any financial contributions to the Taliban from foreign countries (particularly from China, Iran, Russia, and any other foreign country in the Arab Gulf region (or elsewhere) determined relevant by the Director, respectively) made during the year preceding the withdrawal of the United States Armed Forces from Afghanistan on August 31, 2021.

(c) FORM.—The report under subsection (a) may be submitted in classified form, but shall include an unclassified summary.

(d) BIANNUAL UPDATES.—On a biannual basis during the 5-year period following the date of the submission of the report under subsection (a), the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community determined relevant by the Director, shall submit to the congressional intelligence committees an update to such report.

(e) DEFINITIONS.—In this section:

(1) COVERED REGION.—The term ''covered region'' includes the following countries:

(A) China.

(B) The Gulf Cooperation Council countries, including Qatar, Saudi Arabia, the United Arab Emirates.

(C) India.

(D) Iran.

(E) Pakistan.

(F) Tajikistan.

(G) Turkey.

(H) Turkmenistan.

(I) Uzbekistan.

(2) UNITED STATES ENTITY.—The term ''United States entity'' means a citizen of the United States, an embassy or consulate of the United States, or an installation, facility, or personnel of the United States Government.

SEC. 604. REPORT ON THREAT POSED BY EMERGING CHINESE TECHNOLOGY COMPANIES.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Assistant Secretary of the Treasury for Intelligence and Analysis and the Director of the Federal Bureau of Investigation, shall submit

to the congressional intelligence committees a report on the threat to the national security of the United States posed by emerging Chinese technology companies.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment of the threat to the national security of the United States posed by emerging Chinese technology companies, including with respect to—

(A) the practices of the companies and their relationships to the government of China;

(B) the security of the communications, data, and commercial interests of the United States; and

(C) the privacy interests of United States persons.

(2) An assessment of the ability of the United States to counter any such threat, including with respect to different tools that could counter such a threat.

(c) FORM.—The report under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

(d) EMERGING CHINESE TECHNOLOGY COMPANIES DEFINED.—In this section, the term ''emerging Chinese

technology companies'' means a Chinese technology company, including a company listed on the Science and Technology Innovation Board of the Shanghai Stock Exchange, that the Assistant Secretary of the Treasury for Intelligence and Analysis determines poses a significant threat to the national security of the United States.

SEC. 605. REPORT ON COOPERATION BETWEEN CHINA AND UNITED ARAB EMIRATES.

(a) REQUIREMENT.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of elements of the intelligence community that the Director determines appropriate, shall submit to the congressional intelligence committees a report containing the following:

(1) Details on the cooperation between China and the United Arab Emirates regarding defense, security, technology, and other strategically sensitive matters that implicate the national security interests of the United States.

(2) The most recent, as of the date of the report, quarterly assessment by the intelligence community of measures that the United Arab Emirates has implemented to safeguard technology of the United States and the reliability of any assurances by the United Arab Emirates (with respect to both

current assurances and assurances being considered as of the date of the report).

(3) A certification by the Director regarding whether such assurances described in paragraph (2) are viable and sufficient to protect technology of the United States from being transferred to China or other third parties.

(b) FORM.—The report under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

SEC. 606. REPORT ON PROPAGATION OF EXTREMIST IDEOLOGIES FROM SAUDI ARABIA.

(a) REPORT.—Not later than February 1, 2022, the Director of National Intelligence, in consultation with other relevant Federal departments and agencies, shall submit to the congressional intelligence committees a report on the threat of extremist ideologies propagated from Saudi Arabia and the failure of the Government of Saudi Arabia to prevent the propagation of such ideologies. Such report shall include a detailed description of—

(1) the role of governmental and nongovernmental entities and individuals of Saudi Arabia in promoting, funding, and exporting ideologies, including so-called ''Wahhabist ideology'', that inspire extremism or extremist groups in other countries; and

(2) the practical and strategic consequences for vital national security interests of the United States as a result of such promotion, funding, or export.

(b) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 607. REPORT ON EFFECTS OF SANCTIONS BY UNITED STATES.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Assistant Secretary of the Treasury for Intelligence and Analysis, shall submit to the congressional intelligence committees a report on how covered countries respond to sanctions imposed by the United States.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment of whether sanctions imposed by the United States on entities, individuals, or the governments of covered countries have caused those countries to alter their behavior.

(2) An assessment of the effectiveness of—

(A) continuing such sanctions; and

(B) imposing additional sanctions.

(c) FORM.—The report under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

(d) COVERED COUNTRY DEFINED.—In this section, the term ''covered country'' means—

(1) China;

(2) Iran;

(3) Russia; and

(4) any other foreign country the Assistant Secretary of the Treasury for Intelligence and Analysis determines appropriate.

TITLE VII—REPORTS AND OTHER MATTERS

SEC. 701. PILOT PROGRAM FOR SECURITY VETTING OF CERTAIN INDIVIDUALS.

(a) ESTABLISHMENT.—The Under Secretary of Defense for Intelligence and Security may establish a pilot program to identify risks associated with individuals who are performing unclassified research funded by the Department of Defense who would not otherwise undergo Federal personnel vetting.

(b) ELEMENTS.—In carrying out the pilot program under this section, the Under Secretary of Defense for Intelligence and Security may—

(1) identify the size of the population to be vetted under the pilot program;

(2) establish a process to obtain information from individuals to be vetted under the pilot program;

(3) determine the criteria to evaluate national security risks to research funded by the Department of Defense from individuals who are participating in such research;

(4) establish a process to conduct vetting, including referrals to appropriate counterintelligence and law enforcement entities, for the population to be screened under the pilot program; and

(5) carry out the process described in paragraph (4) with respect to the population to be screened under the pilot program.

(c) REPORT.—Before commencing the pilot program under this section, the Under Secretary of Defense for Intelligence and Security shall submit to the appropriate congressional committees a report containing details of the planned elements of the pilot program under subsection (b).

(d) BRIEFINGS.—Not less frequently than annually during the 3-year period beginning on the date that is 1 year after the date of the enactment of this Act, the Under

Secretary of Defense for Intelligence and Security shall provide to the appropriate congressional committees a briefing on the status of the pilot program under this section.

(e) TERMINATION.—The authority to conduct the pilot program under this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

(f) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the congressional intelligence committees; and

(2) the congressional defense committees (as such term is defined in section 101(a) of title 10, United States Code).

SEC. 702. INTELLIGENCE ASSESSMENT AND REPORTS ON FOREIGN RACIALLY MOTIVATED VIOLENT EXTREMISTS.

(a) INTELLIGENCE ASSESSMENT.—

(1) REQUIREMENT.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence, acting through the Director of the National Counterterrorism Center, in coordination with the Director of the Federal Bu-

reau of Investigation and the Under Secretary of Homeland Security for Intelligence and Analysis, and in consultation with other relevant Federal departments and agencies, shall submit to the appropriate congressional committees an intelligence assessment on significant threats to the United States associated with foreign racially motivated violent extremist organizations.

(2) ELEMENTS.—The assessment under paragraph (1) shall include the following:

(A) A list of foreign racially motivated violent extremist organizations that pose a significant threat to the national security of the United States.

(B) With respect to each such organization—

(i) an overview of the membership, ideology, and activities;

(ii) a description of any transnational links to the United States or United States persons;

(iii) a description of the leadership, plans, intentions, and capabilities;

(iv) whether (and if so, to what extent) foreign governments or their proxies

provide any manner of support to such organizations, including a list of each such foreign government or proxy;

(v) a description of the composition and characteristics of the members and support networks, including whether (and if so, to what extent) the members are also a part of a military, security service, or police;

(vi) a description of financing and other forms of material support;

(vii) an assessment of trends and patterns relative to communications, travel, and training (including whether and to what extent the organization is engaged in or facilitating military or paramilitary training);

(viii) an assessment of the radicalization and recruitment, including an analysis of the extremist messaging motivating members and supporters; and

(ix) whether (and if so, to what extent) foreign governments have sufficient laws and policies to counter threats to the

United States associated with the organization, including best practices and gaps.

(C) An assessment of the status and extent of information sharing, intelligence partnerships, foreign police cooperation, and mutual legal assistance between the United States and foreign governments relative to countering threats to the United States associated with foreign racially motivated violent extremist organizations.

(D) An assessment of intelligence gaps and recommendations on how to remedy such gaps.

(E) An opportunity analysis regarding countering such threats, including, at a minimum, with respect to mitigating and disrupting the transnational nexus.

(3) STANDARDS.—The intelligence assessment under paragraph (1) shall be conducted in a manner that meets the analytic integrity and tradecraft standards of the intelligence community.

(4) FORM.—The intelligence assessment under paragraph (1) shall be submitted in unclassified form, but may include a classified annex in electronic form that is fully indexed and searchable. In

carrying out this paragraph, the officials specified in paragraph (1) shall—

(A) ensure that the assessment is unclassified to the extent possible; and

(B) ensure that the assessment is drafted in a way to maximize the ability to share the assessment, including the classified annex, with the entities under paragraph (5).

(5) SHARING.—Consistent with the protection of classified information, the Director of National Intelligence, acting through the Director of the National Counterterrorism Center, in coordination with the Director of the Federal Bureau of Investigation and the Under Secretary of Homeland Security for Intelligence and Analysis, shall share the intelligence assessment under paragraph (1) with—

(A) appropriate Federal departments and agencies;

(B) Joint Terrorism Task Forces and the Domestic Terrorism-Hate Crimes Fusion Cell of the Federal Bureau of Investigation;

(C) State, local, and Tribal law enforcement officials, including officials who operate within State, local, and regional fusion centers through the Department of Homeland Security

State, Local, and Regional Fusion Center Initiative established in accordance with section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h); and

(D) appropriate foreign governments, including foreign intelligence services and foreign police, and international institutions, that partner with the United States on countering significant threats associated with foreign racially motivated violent extremist organizations.

(b) REPORT.—

(1) REQUIREMENT.—Not later than 150 days after the date of the enactment of this Act, the Director of National Intelligence (acting through the Director of the National Counterterrorism Center), in coordination with the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Homeland Security, and in a manner consistent with the authorities and responsibilities of such Secretary or Director, shall submit to the appropriate congressional committees a report on the use of Federal laws, regulations, and policies by the Federal Government to counter significant threats to the United States and United States persons associ-

ated with foreign racially motivated violent extremist organizations.

(2) ELEMENTS.—The report under paragraph shall include the following:

(A) An identification, description, and assessment of the use and efficacy of, Federal laws, regulations, and policies used by the Federal Government to address significant threats to the United States and United States persons associated with foreign racially motivated violent extremist organizations, including pursuant to—

(i) section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) and section 119 of the National Security Act of 1949 (50 U.S.C. 3056), particularly with respect to the coordination and integration of all instruments of national power;

(ii) Executive Order 12333 (50 U.S.C. 3001 note), as amended;

(iii) the designation of foreign terrorist organizations under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189);

(iv) the designation of specially designated terrorists, specially designated global terrorists, or specially designated nationals and blocked persons, pursuant to Executive Orders 13886, 13372, and 13224 and parts 594, 595, 596, and 597 of title 31, Code of Federal Regulations;

(v) National Security Presidential Memorandums 7 and 9, particularly with respect to the sharing of terrorism information and screening and vetting activities; and

(vi) any other applicable Federal laws, regulations, or policies.

(B) An assessment of whether (and if so, to what extent and why) such Federal laws, regulations, and policies are sufficient to counter such threats, including a description of any gaps and specific examples to illustrate such gaps.

(C) Recommendations regarding how to remedy the gaps under subparagraph (B).

(3) PRIVACY AND CIVIL LIBERTIES ASSESSMENT.—Not later than 180 days after the date of the enactment of this Act, the Privacy and Civil Lib-

erties Oversight Board, in consultation with the civil liberties and privacy officers of the Federal departments and agencies the Board determines appropriate, shall submit to the appropriate congressional committees a report containing—

(A) an assessment of the impacts on the privacy and civil liberties of United States persons concerning the use or recommended use of any Federal laws, regulations, and policies specified in paragraph (2); and

(B) recommendations on options to develop protections to mitigate such impacts.

(4) FORM.—The reports under paragraphs (1) and (2) shall be submitted in unclassified form, but may include a classified annex in electronic form that is fully indexed and searchable. In carrying out this paragraph, the officials responsible for submitting such reports shall ensure that the reports are unclassified to the extent possible.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Permanent Select Committee on Intelligence, the Committee on Homeland Secu-

rity, the Committee on Foreign Affairs, and the Committee on the Judiciary of the House of Representatives; and

(B) the Select Committee on Intelligence, the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, and the Committee on the Judiciary of the Senate.

(2) TERRORISM INFORMATION.—The term ''terrorism information'' has the meaning given that term in section 1016(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(a)).

(3) UNITED STATES PERSON.—The term ''United States person'' has the meaning given that term in section 105A(c) of the National Security Act of 1947 (50 U.S.C. 3039).

SEC. 703. PERIODIC REPORT ON POSITIONS IN THE INTELLIGENCE COMMUNITY THAT CAN BE CONDUCTED WITHOUT ACCESS TO CLASSIFIED INFORMATION, NETWORKS, OR FACILITIES.

Section 6610 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3352e) is amended—

(1) by striking ''this Act and not less frequently than once every 5 years thereafter,'' and inserting ''this Act, and biennially thereafter,''; and

(2) by adding at the end the following new sentence: ''Such report shall take into account the potential effect of maintaining continuity of operations during a covered national emergency (as defined by section 303 of the Intelligence Authorization Act for Fiscal Year 2021 (division W of Public Law 116–260)) and the assessed needs of the intelligence community to maintain such continuity of operations.''.

SEC. 704. BIENNIAL REPORTS ON FOREIGN BIOLOGICAL THREATS.

(a) REQUIREMENT.—Title XI of the National Security Act of 1947 (50 U.S.C. 3231 et seq.) is amended by adding at the end the following new section (and conforming the table of contents at the beginning of such Act accordingly):

''SEC. 1111. BIENNIAL REPORTS ON FOREIGN BIOLOGICAL THREATS.

''(a) REPORTS.—On a biennial basis until the date that is 10 years after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, the Director of National Intelligence shall submit to the congressional intelligence committees a comprehensive report

on the activities, prioritization, and responsibilities of the intelligence community with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country.

"(b) MATTERS INCLUDED.—Each report under subsection (a) shall include, with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country, the following:

"(1) A detailed description of all activities relating to such threats undertaken by each element of the intelligence community, and an assessment of any gaps in such activities.

"(2) A detailed description of all duties and responsibilities relating to such threats explicitly authorized or otherwise assigned, exclusively or jointly, to each element of the intelligence community, and an assessment of any identified gaps in such duties or responsibilities.

"(3) A description of the coordination among the relevant elements of the intelligence community with respect to the activities specified in paragraph (1) and the duties and responsibilities specified in paragraph (2).

"(4) An inventory of the strategies, plans, policies, and interagency agreements of the intelligence

community relating to the collection, monitoring, analysis, mitigation, and attribution of such threats, and an assessment of any identified gaps therein.

''(5) A description of the coordination and interactions among the relevant elements of the intelligence community and non-intelligence community partners.

''(6) An assessment of foreign malign influence efforts relating to such threats, and a description of how the intelligence community contributes to efforts by non-intelligence community partners to counter such foreign malign influence.

''(c) FORM.—Each report submitted under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

''(d) DEFINITIONS.—In this section:

''(1) COVERED COUNTRY.—The term 'covered country' means—

''(A) China;

''(B) Iran;

''(C) North Korea;

''(D) Russia; and

''(E) any other foreign country—

"(i) from which the Director of National Intelligence determines a biological threat emanates; or

"(ii) that the Director determines has a known history of, or has been assessed as having conditions present for, infectious disease outbreaks or epidemics.

"(2) FOREIGN BIOLOGICAL THREAT.—The term 'foreign biological threat' means biological warfare, bioterrorism, naturally occurring infectious diseases, or accidental exposures to biological materials, without regard to whether the threat originates from a state actor, a non-state actor, natural conditions, or an undetermined source.

"(3) FOREIGN MALIGN INFLUENCE.—The term 'foreign malign influence' has the meaning given such term in section 119C(e).

"(4) NON-INTELLIGENCE COMMUNITY PARTNER.—The term 'non-intelligence community partner' means a Federal department or agency that is not an element of the intelligence community.".

(b) FIRST REPORT.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees the first report required under section

1111 of the National Security Act of 1947, as added by subsection (a).

SEC. 705. ANNUAL REPORTS ON DOMESTIC ACTIVITIES OF THE INTELLIGENCE COMMUNITY.

(a) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) the Federal Bureau of Investigation and the Department of Homeland Security conduct vital work in enforcing the rule of law and safeguarding the people of the United States from harm;

(2) the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 118 Stat. 3638) sought to facilitate greater information sharing between law enforcement and intelligence communities for the purpose of thwarting attacks on the homeland from international terrorist organizations;

(3) National Intelligence Program funds should be expended only in support of intelligence activities with a foreign nexus, consistent with the definition of ''intelligence'' provided by Congress in section 3 of the National Security Act of 1947 (50 U.S.C. 3003); and

(4) the intelligence community should not engage in the collection, assessment, or analysis of in-

formation that pertains exclusively to United States persons absent a foreign nexus.

(b) REQUIREMENT.—Title XI of the National Security Act of 1947 (50 U.S.C. 3231 et seq.), as amended by section 704, is further amended by adding at the end the following new section (and conforming the table of contents at the beginning of such Act accordingly):

"SEC. 1112. ANNUAL REPORTS ON THE DOMESTIC ACTIVITIES OF THE INTELLIGENCE COMMUNITY.

"(a) REPORTS.—Not later than January 31 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report—

"(1) identifying all domestic activities undertaken by each element of the intelligence community during the prior fiscal year; and

"(2) for each activity identified under paragraph (1), a statement of the legal authority authorizing such activity to be undertaken.

"(b) FORM.—Each report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.".

(c) FIRST REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees the first report required under section 1112

of the National Security Act of 1947, as added by subsection (a).

SEC. 706. ANNUAL REPORTS ON CERTAIN CYBER VULNERABILITIES PROCURED BY INTELLIGENCE COMMUNITY AND FOREIGN COMMERCIAL PROVIDERS OF CYBER VULNERABILITIES.

(a) REQUIREMENT.—Title XI of the National Security Act of 1947 (50 U.S.C. 3231 et seq.), as amended by section 705, is further amended by adding at the end the following new section (and conforming the table of contents at the beginning of such Act accordingly):

"SEC. 1113. ANNUAL REPORTS ON CERTAIN CYBER VULNERABILITIES PROCURED BY INTELLIGENCE COMMUNITY AND FOREIGN COMMERCIAL PROVIDERS OF CYBER VULNERABILITIES.

"(a) ANNUAL REPORTS.—On an annual basis through 2026, the Director of the Central Intelligence Agency and the Director of the National Security Agency, in coordination with the Director of National Intelligence, shall jointly submit to the congressional intelligence committees a report containing information on foreign commercial providers and the cyber vulnerabilities procured by

the intelligence community through foreign commercial providers.

''(b) ELEMENTS.—Each report under subsection (a) shall include, with respect to the period covered by the report, the following:

''(1) A description of each cyber vulnerability procured through a foreign commercial provider, including—

''(A) a description of the vulnerability;

''(B) the date of the procurement;

''(C) whether the procurement consisted of only that vulnerability or included other vulnerabilities;

''(D) the cost of the procurement;

''(E) the identity of the commercial provider and, if the commercial provider was not the original supplier of the vulnerability, a description of the original supplier;

''(F) the country of origin of the vulnerability; and

''(G) an assessment of the ability of the intelligence community to use the vulnerability, including whether such use will be operational or for research and development, and the approximate timeline for such use.

"(2) An assessment of foreign commercial providers that—

"(A) pose a significant threat to the national security of the United States; or

"(B) have provided cyber vulnerabilities to any foreign government that—

"(i) has used the cyber vulnerabilities to target United States persons, the United States Government, journalists, or dissidents; or

"(ii) has an established pattern or practice of violating human rights or suppressing dissent.

"(3) An assessment of whether the intelligence community has conducted business with the foreign commercial providers identified under paragraph (2) during the 5-year period preceding the date of the report.

"(c) FORM.—Each report under subsection (a) may be submitted in classified form.

"(d) DEFINITIONS.—In this section:

"(1) COMMERCIAL PROVIDER.—The term 'commercial provider' means any person that sells, or acts as a broker, for a cyber vulnerability.

''(2) CYBER VULNERABILITY.—The term 'cyber vulnerability' means any tool, exploit, vulnerability, or code that is intended to compromise a device, network, or system, including such a tool, exploit, vulnerability, or code procured by the intelligence community for purposes of research and development.''.

(b) FIRST REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency and the Director of the National Security Agency shall jointly submit to the appropriate congressional committees the first report required under section 1113 of the National Security Act of 1947, as added by subsection (a).

SEC. 707. IMPROVEMENTS TO ANNUAL REPORT ON DEMOGRAPHIC DATA OF EMPLOYEES OF INTELLIGENCE COMMUNITY.

Section 5704(c) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334b(c)) is amended—

(1) in the matter preceding paragraph (1), by striking ''After making available a report under subsection (b), the Director of National Intelligence shall annually provide a report'' and inserting ''Not

later than March 31 of each year, the Director of National Intelligence shall provide a report''; and

(2) by striking paragraph (1) and inserting the following new paragraph:

''(1) demographic data and information on the status of diversity and inclusion efforts of the intelligence community, including demographic data relating to—

''(A) the average years of service;

''(B) the average number of years of service for each level in the General Schedule, Senior Executive Service, Senior Intelligence Service, or equivalent; and

''(C) career categories.''.

SEC. 708. NATIONAL INTELLIGENCE ESTIMATE ON ESCALATION AND DE-ESCALATION OF GRAY ZONE ACTIVITIES IN GREAT POWER COMPETITION.

(a) FINDINGS.—Congress finds the following:

(1) The conventional power of the United States has driven foreign adversaries to a level of competition that does not always depend on military confrontation with the United States.

(2) Rather than challenging the United States in a manner that could provoke a kinetic military response, foreign adversaries of the United States have

turned to carrying out gray zone activities to advance the interests of such adversaries, weaken the power of the United States, and erode the norms that underpin the United States-led international order.

(3) Gray zone activity falls on a spectrum of attribution and deniability that ranges from covert adversary operations, to detectible covert adversary operations, to unattributable adversary operations, to deniable adversary operations, to open adversary operations.

(4) To adequately address such a shift to gray zone activity, the United States must understand what actions tend to either escalate or de-escalate such activity by our adversaries.

(5) The laws, principles, and values of the United States are strategic advantages in great power competition with authoritarian foreign adversaries that carry out gray zone activities, because such laws, principles, and values increase the appeal of the governance model of the United States, and the United States-led international order, to states and peoples around the world.

(6) The international security environment has demonstrated numerous examples of gray zone ac-

tivities carried out by foreign adversaries, including the following activities of foreign adversaries:

(A) Information operations, such as efforts by Russia to influence the 2020 United States Federal elections (as described in the March 15, 2021, intelligence community assessment of the Office of the Director of National Intelligence made publicly available on March 15, 2021).

(B) Adversary political coercion operations, such as the wielding of energy by Russia, particularly in the context of Ukrainian gas pipelines, to coerce its neighbors into compliance with its policies.

(C) Cyber operations, such as the use by China of cyber tools to conduct industrial espionage.

(D) Provision of support to proxy forces, such as the support provided by Iran to Hezbollah and Shia militia groups.

(E) Provocation by armed forces controlled by the government of the foreign adversary through measures that do not rise to the level of an armed attack, such as the use of the China Coast Guard and maritime militia by

China to harass the fishing vessels of other countries in the South China Sea.

(F) Alleged uses of lethal force on foreign soil, such as the 2018 attempts by Russia to poison Sergei Skripal in London.

(G) The potential use by an adversary of technology that causes anomalous health incidents among United States Government personnel.

(b) NATIONAL INTELLIGENCE ESTIMATE.—

(1) REQUIREMENT.—The Director of National Intelligence, acting through the National Intelligence Council, shall produce a National Intelligence Estimate on how foreign adversaries use gray zone activities to advance interests, what responses by the United States (or the allies or partners of the United States) would tend to result in the escalation or de-escalation of such gray zone activities by foreign adversaries, and any opportunities for the United States to minimize the extent to which foreign adversaries use gray zone activities in furtherance of great power competition.

(2) MATTERS INCLUDED.—To the extent determined appropriate by the National Intelligence Council, the National Intelligence Estimate produced

under paragraph (1) may include an assessment of the following topics:

(A) Any potential or actual lethal or harmful gray zone activities carried out against the United States by foreign adversaries, including against United States Government employees and United States persons, whether located within or outside of the United States.

(B) To the extent such activities have occurred, or are predicted to occur—

(i) opportunities to reduce or deter any such activities; and

(ii) any actions of the United States Government that would tend to result in the escalation or de-escalation of such activities.

(C) Any incidents in which foreign adversaries could have used, but ultimately did not use, gray zone activities to advance the interests of such adversaries, including an assessment as to why the foreign adversary ultimately did not use gray zone activities.

(D) The effect of lowering the United States Government threshold for the public attribution of detectible covert adversary oper-

ations, unattributable adversary operations, and deniable adversary operations.

(E) The effect of lowering the United States Government threshold for responding to detectible covert adversary operations, unattributable adversary operations, and deniable adversary operations.

(F) The extent to which the governments of foreign adversaries exercise control over any proxies or parastate actors used by such governments in carrying out gray zone activities.

(G) The extent to which gray zone activities carried out by foreign adversaries affect the private sector of the United States.

(H) The international norms that provide the greatest deterrence to gray zone activities carried out by foreign adversaries, and opportunities for strengthening those norms.

(I) The effect, if any, of the strengthening of democratic governance abroad on the resilience of United States allies and partners to gray zone activities.

(J) Opportunities to strengthen the resilience of United States allies and partners to

gray zone activities, and associated tactics, carried out by foreign adversaries.

(K) Opportunities for the United States to improve the detection of, and early warning for, such activities and tactics.

(L) Opportunities for the United States to galvanize international support in responding to such activities and tactics.

(3) SUBMISSION TO CONGRESS.—

(A) SUBMISSION.—Not later than 1 year after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees the National Intelligence Estimate produced under paragraph (1), including all intelligence reporting underlying the Estimate.

(B) NOTICE REGARDING SUBMISSION.—If at any time before the deadline specified in subparagraph (A), the Director determines that the National Intelligence Estimate produced under paragraph (1) cannot be submitted by such deadline, the Director shall (before such deadline) submit to the congressional intelligence committees a report setting forth the reasons why the National Intelligence Estimate cannot

be submitted by such deadline and an estimated date for the submission of the National Intelligence Estimate.

(C) FORM.—Any report under subparagraph (B) shall be submitted in unclassified form.

(4) PUBLIC VERSION.—Consistent with the protection of intelligence sources and methods, at the same time as the Director submits to the congressional intelligence committees the National Intelligence Estimate under paragraph (1), the Director shall make publicly available on the internet website of the Director an unclassified version of the key findings of the National Intelligence Estimate.

(5) DEFINITIONS.—In this subsection:

(A) GRAY ZONE ACTIVITY.—The term ''gray zone activity'' means an activity to advance the national interests of a State that—

(i) falls between ordinary statecraft and open warfare;

(ii) is carried out with an intent to maximize the advancement of interests of the state without provoking a kinetic military response by the United States; and

(iii) falls on a spectrum that ranges from covert adversary operations, to detectible covert adversary operations, to unattributable adversary operations, to deniable adversary operations, to open adversary operations.

(B) COVERT ADVERSARY OPERATION.—The term ''covert adversary operation'' means an operation by an adversary that—

(i) the adversary intends to remain below the threshold at which the United States detects the operation; and

(ii) does stay below such threshold.

(C) DETECTIBLE COVERT ADVERSARY OPERATION.—The term ''detectible covert adversary operation'' means an operation by an adversary that—

(i) the adversary intends to remain below the threshold at which the United States detects the operation; but

(ii) is ultimately detected by the United States at a level below the level at which the United States will publicly attribute the operation to the adversary.

(D) UNATTRIBUTABLE ADVERSARY OPERATION.—The term ''unattributable adversary operation'' means an operation by an adversary that the adversary intends to be detected by the United States, but remain below the threshold at which the United States will publicly attribute the operation to the adversary.

(E) DENIABLE ADVERSARY OPERATION.—The term ''deniable adversary operation'' means an operation by an adversary that—

(i) the adversary intends to be detected and publicly or privately attributed by the United States; and

(ii) the adversary intends to deny, to limit the response by the United States, and any allies of the United States.

(F) OPEN ADVERSARY OPERATION.—The term ''open adversary operation'' means an operation by an adversary that the adversary openly acknowledges as attributable to the adversary.

(c) REQUIREMENT TO DEVELOP LEXICON.—

(1) REQUIREMENT.—The Director of National Intelligence, acting through the National Intelligence Council, shall develop a lexicon of common terms

(and corresponding definitions for such terms) for concepts associated with gray zone activities.

(2) CONSIDERATIONS.—In developing the lexicon under paragraph (1), the National Intelligence Council shall include in the lexicon each term (and the corresponding definition for each term) specified in subsection (b)(5), unless the National Intelligence Council determines that an alternative term (or alternative definition)—

(A) more accurately describes a concept associated with gray zone activities; or

(B) is preferable for any other reason.

(3) REPORT.—

(A) PUBLICATION.—The Director of National Intelligence shall publish a report containing the lexicon developed under paragraph (1).

(B) FORM.—The report under subparagraph (A) shall be published in unclassified form.

SEC. 709. REPORT ON CERTAIN ACTIONS TAKEN BY INTELLIGENCE COMMUNITY WITH RESPECT TO HUMAN RIGHTS AND INTERNATIONAL HUMANITARIAN LAW.

(a) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, the Director of the National Security Agency, the Secretary of Defense, and the Director of the Defense Intelligence Agency, shall submit to the congressional intelligence committees a report on certain actions taken by the intelligence community with respect to human rights and international humanitarian law.

(b) ELEMENTS.—The report under subsection (a) shall include the following:

(1) A detailed explanation of whether, and to what extent, each element of the intelligence community has provided intelligence products relating to the efforts of the Secretary of State and the Secretary of Treasury regarding the categorization, determinations on eligibility for assistance and training, and general understanding, of covered entities that commit, engage, or are otherwise complicit in, violations of human rights or international humanitarian law.

(2) A detailed explanation of whether, and to what extent, each element of the intelligence community has provided intelligence products relating to any of the following:

(A) Section 7031(c) of the Department of State, Foreign Operations, and Related Programs Appropriations Act, 2020 (division G of Public Law 116–94; 8 U.S.C. 1182 note).

(B) The visa restriction policy of the Department of State announced on February 26, 2021, and commonly referred to as the ''Khashoggi Ban''.

(C) The annual report requirement of the Department of Defense under section 1057 of the National Defense Authorization Act for Fiscal Year 2018 (131 Stat. 1572).

(D) The Global Magnitsky Human Rights Accountability Act (subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note).

(3) A detailed explanation of the following processes:

(A) The process of each element of the intelligence community for monitoring covered entities for derogatory human rights or international humanitarian law information.

(B) The process of each element of the intelligence community for determining the credibility of derogatory human rights or international humanitarian law information.

(C) The process of each element of the intelligence community for determining what further action is appropriate if derogatory human rights or international humanitarian law information is determined to be credible.

(4) An unredacted copy of each policy or similar document that describes a process specified in paragraph (3).

(5) A detailed explanation of whether, with respect to each element of the intelligence community, the head of the element has changed or restricted any activities of the element in response to derogatory human rights or international humanitarian law information.

(6) Examples of any changes or restrictions specified in paragraph (5) taken by the head of the element of the intelligence community during the two years preceding the date of the submission of the report.

(c) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) DEFINITIONS.—In this section:

(1) COVERED ENTITY.—The term ''covered entity''—

(A) means an individual, unit, or foreign government that—

(i) has a cooperative relationship with the United States Government; or

(ii) is the target of an intelligence collection activity carried out by the United States Government; but

(B) does not include an employee of the United States Government.

(2) DEROGATORY HUMAN RIGHTS OR INTERNATIONAL HUMANITARIAN LAW INFORMATION.—The term ''derogatory human rights or international humanitarian law information'' means information tending to suggest that a covered entity committed, participated, or was otherwise complicit in, a violation of human rights or international humanitarian law, regardless of the credibility of such information, the source of the information, or the level of classification of the information.

(3) VIOLATION OF HUMAN RIGHTS OR INTERNATIONAL HUMANITARIAN LAW.—The term ''violation of human rights or international humanitarian law'' includes a violation of any authority or obligation of the United States Government related to human rights or international humanitarian law, without regard to whether such authority or obligation is codified in a provision of law, regulation, or policy.

SEC. 710. BRIEFING ON TRAININGS RELATING TO BLOCKCHAIN TECHNOLOGY.

(a) BRIEFING.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall provide to the congressional intelligence committees a briefing on the feasibility and benefits of providing training described in subsection (b).

(b) TRAINING DESCRIBED.—Training described in this subsection is training that meets the following criteria:

(1) The training is on cryptocurrency, blockchain technology, or both subjects.

(2) The training may be provided through partnerships with universities or private sector entities.

SEC. 711. REPORT ON PROSPECTIVE ABILITY TO ADMINISTER COVID–19 VACCINES AND OTHER MEDICAL INTERVENTIONS TO CERTAIN INTELLIGENCE COMMUNITY PERSONNEL.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence and the Under Secretary of Defense for Intelligence and Security, in consultation with the elements of the intelligence community and relevant public health agencies of the United States, shall jointly develop and submit to the congressional intelligence committees a report on the prospective ability of the intelligence community to administer COVID–19 vaccines, and such other medical interventions as may be relevant in the case of a future covered national emergency, to covered personnel (particularly with respect to essential covered personnel and covered personnel deployed outside of the United States).

(b) MATTERS INCLUDED.—The report under subsection (a) shall include an assessment of the following:

(1) The prospective ability of the elements of the intelligence community to administer COVID–19 vaccines (including subsequent booster shots for COVID–19), to covered personnel, and whether additional authorities or resources are necessary for, or may otherwise facilitate, such administration.

(2) The potential risks and benefits of granting the additional authorities or resources described in paragraph (1) to the Director, the Under Secretary, or both.

(3) With respect to potential future covered national emergencies, including future outbreaks of an infectious pandemic disease or similar public health emergencies, the following:

(A) The ability of the intelligence community to ensure the timely administration of medical interventions to covered personnel during the covered national emergency.

(B) Whether additional authorities or resources are necessary to ensure, or may otherwise facilitate, such timely administration, including with respect to the ability of the Director or Under Secretary to provide an alternative means of access to covered personnel with reduced access to the interventions provided by the respective element.

(C) The potential risks and benefits of granting the additional authorities or resources described in subparagraph (B) to the Director, the Under Secretary, or both.

(4) A summary of the findings of the survey under subsection (c).

(c) SURVEY.—Not later than 120 days after the date of the enactment of this Act, and prior to submitting the report under subsection (a), the Director and the Under Secretary shall jointly conduct a survey to determine the process by which each element of the intelligence community has administered COVID–19 vaccines to covered personnel, to inform continued medical care relating to COVID–19 and future responses to covered national emergencies. Such survey shall address, with respect to each element, the following:

(1) The timeline of the element with respect to the administration of COVID–19 vaccines prior to the date of the enactment of this Act.

(2) The process by which the element determined when covered personnel would become eligible to receive the COVID–19 vaccine (including if certain categories of such personnel became eligible before others).

(3) A general approximation of the percentage of covered personnel of the element that received the COVID–19 vaccine from the element versus through an alternative means (such as a private sector entity, foreign government, State, or local government),

particularly with respect to covered personnel deployed outside of the United States.

(4) Any challenges encountered by the element with respect to the administration of COVID–19 vaccines prior to the date of the enactment of this Act.

(5) Any other feedback determined relevant for purposes of the survey.

(d) PRIVACY CONSIDERATIONS.—In carrying out the report and survey requirements under this section, the Director, the Under Secretary, and the heads of the elements of the intelligence community shall ensure, to the extent practicable, the preservation of medical privacy and the anonymity of data.

(e) DEFINITIONS.—In this section:

(1) COVERED NATIONAL EMERGENCY.—The term ''covered national emergency'' has the meaning given such term in section 303 of the Intelligence Authorization Act for Fiscal Year 2021 (50 U.S.C. 3316b).

(2) COVERED PERSONNEL.—The term ''covered personnel'' means personnel who are—

(A) employees of, or otherwise detailed or assigned to, an element of the intelligence community; and

(B) funded under the National Intelligence Program or the Military Intelligence Program.

(3) ESSENTIAL COVERED PERSONNEL.—The term ''essential covered personnel'' means covered personnel deemed essential to—

(A) continuity of operations of the intelligence community;

(B) continuity of operations of the United States Government; or

(C) other purposes related to the national security of the United States.

(4) NATIONAL INTELLIGENCE PROGRAM.—The term ''National Intelligence Program'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 712. REPORT ON POTENTIAL INCLUSION WITHIN INTELLIGENCE COMMUNITY OF THE OFFICE OF NATIONAL SECURITY OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Secretary of Health and Human Services, shall submit to the appropriate congressional committees a report on the potential advantages and disadvantages of adding the Office of National Secu-

rity of the Department of Health and Human Services as a new element of the intelligence community.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment of the following:

(A) The likelihood that the addition of the Office of National Security as a new element of the intelligence community would increase connectivity between other elements of the intelligence community working on health security topics and the Department of Health and Human Services.

(B) The likelihood that such addition would increase the flow of raw intelligence and finished intelligence products to officials of the Department of Health and Human Services.

(C) The likelihood that such addition would facilitate the flow of information relating to health security topics to intelligence analysts of various other elements of the intelligence community working on such topics.

(D) The extent to which such addition would clearly demonstrate to both the national security community and the public health community that health security is national security.

(E) Any anticipated impediments to such addition relating to additional budgetary oversight by the executive branch or Congress.

(F) Any other significant advantages or disadvantages of such addition, as identified by either the Director of National Intelligence or the Secretary of Health and Human Services.

(2) A joint recommendation by the Director of National Intelligence and the Secretary of Health and Human Services as to whether to add the Office of National Security as a new element of the intelligence community.

(c) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the congressional intelligence committees; and

(2) the Committee on Energy and Commerce of the House of Representatives and the Committee on Health, Education, Labor, and Pensions of the Senate.

SEC. 713. REPORTS RELATING TO INSPECTOR GENERAL OF DEFENSE INTELLIGENCE AGENCY.

(a) REPORT ON RESPONSES BY INSPECTOR GENERAL TO SUBSTANTIATED ALLEGATIONS.—

(1) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of the Defense Intelligence Agency shall submit to the congressional intelligence committees a report on allegations of reprisal or abuse of authority determined to be substantiated by the Inspector General of the Defense Intelligence Agency during the 5-year period preceding the date of the enactment of this Act.

(2) MATTERS INCLUDED.—The report under paragraph (1) shall include, with respect to each allegation determined to be substantiated during the 5-year period specified in such paragraph, a description of the following:

(A) Details of each substantiated allegation.

(B) The rank or grade of the individuals involved in the allegation.

(C) Any disciplinary action recommended by the Inspector General in response to the allegation, or, if the Inspector General recommended no disciplinary action be taken in re-

sponse, any justification for such recommendation.

(D) Any disciplinary action taken by the relevant manager of the Defense Intelligence Agency in response to the allegation.

(E) Whether the relevant manager reduced, or declined to take, a disciplinary action recommended by the Inspector General in response to the allegation.

(F) Any justification from the relevant manager regarding the decision to take, reduce, or decline to take, a disciplinary action recommended by the Inspector General in response to the allegation.

(G) The process by which Defense Intelligence Agency management reviews and makes decisions regarding disciplinary actions in response to substantiated allegations, including—

(i) the criteria applied by management in making the decision to take, reduce, or decline to take, a disciplinary action;

(ii) a description of which managers have the authority to make such decisions, including the rank or grade of the managers; and

(iii) a description of any formal or informal appeals processes available with respect to such decisions.

(3) FORM.—The report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(b) REPORT ON PROCESSES FOR ENSURING INDEPENDENCE OF INSPECTOR GENERAL.—

(1) REPORT.—Not later than 30 days after the date of the enactment of this Act, the Director of the Defense Intelligence Agency shall submit to the congressional intelligence committees and the Council of the Inspectors General on Integrity and Efficiency established under section 11 of the Inspector General Act of 1978 (5 U.S.C. App.) a report on the processes of the Defense Intelligence Agency for ensuring the independence of the position of the Inspector General of the Defense Intelligence Agency.

(2) MATTERS INCLUDED.—The report under paragraph (1) shall include a description of the following:

(A) The selection criteria used by the Director in the appointment of the Inspector General.

(B) The methods used by the Director to ensure the independence of the position of the Inspector General, including—

(i) the process for vetting candidates for such position for independence from leadership of the Defense Intelligence Agency and from officials occupying positions in the Defense Intelligence Senior Executive Service; and

(ii) the process for evaluating such candidates for conflicts of interest.

(3) FORM.—The report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(c) ASSESSMENT BY COUNCIL OF INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY.—

(1) ASSESSMENT.—Not later than 120 days after the date of the enactment of this Act, the Council of the Inspectors General on Integrity and Efficiency shall—

(A) conduct an assessment of the effectiveness of the selection criteria and methods specified in subsection (b)(2) with respect to the position of the Inspector General of the Defense Intelligence Agency; and

(B) submit to the congressional intelligence committees a report containing the results of such assessment.

(2) FORM.—The report under paragraph (1)(B) shall be submitted in unclassified form, but may include a classified annex.

SEC. 714. REPORT ON RARE EARTH ELEMENTS.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Director of the Defense Intelligence Agency, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, and any other head of an element of the intelligence community that the Director of National Intelligence determines relevant, shall submit to the congressional intelligence committees a report on rare earth elements.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment coordinated by the National Intelligence Council of—

(A) long-term trends in the global rare earth element industry;

(B) the national security, economic, and industrial risks to the United States, and to the partners and allies of the United States, with

respect to relying on foreign countries for rare earth mining and the processing or production of rare earth elements;

(C) the intentions of foreign governments with respect to limiting, reducing, or ending access of the United States or the partners and allies of the United States to—

(i) rare earth elements; or

(ii) any aspect of the rare earth mining, processing, or production chain; and

(D) opportunities for the United States, and for the partners and allies of the United States, to assure continued access to—

(i) rare earth elements; and

(ii) the rare earth mining, processing, or production chain.

(2) A description of—

(A) any relevant procurement, use, and supply chain needs of the intelligence community with respect to rare earth elements;

(B) any relevant planning or efforts by the intelligence community to assure secured access to rare earth magnets;

(C) any assessed vulnerabilities or risks to the intelligence community with respect to rare earth elements;

(D) any relevant planning or efforts by the intelligence community to coordinate with departments and agencies of the United States Government that are not elements of the intelligence community on securing the rare earth element supply chain; and

(E) any previous or anticipated efforts by the Supply Chain and Counterintelligence Risk Management Task Force established under section 6306 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3370) with respect to rare earth elements.

(c) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) RARE EARTH ELEMENTS DEFINED.—In this section, the term ''rare earth elements'' includes products that contain rare earth elements, including rare earth magnets.

SEC. 715. REPORT ON PLAN TO FULLY FUND THE INFORMATION SYSTEMS SECURITY PROGRAM AND NEXT GENERATION ENCRYPTION.

(a) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Defense shall submit to the appropriate congressional committees a report on the resources necessary to fully fund the Information Systems Security Program during the period covered by the most recent future-years defense program submitted under section 221 of title 10, United States Code—

(1) to address the cybersecurity requirements of the Department of Defense; and

(2) for the adoption of next generation encryption into existing and future systems.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment by the Chief Information Officer of the Department of Defense, in coordination with the chiefs of the Armed Forces and in consultation with the Director of the National Security Agency, of the additional resources required to fund the Information Systems Security Program at a level that satisfies current and anticipated cybersecurity requirements of the Department.

(2) An identification of any existing funding not currently aligned to the Program that is more appropriately funded through the Program.

(3) A strategic plan, developed in coordination with the chiefs of the Armed Forces and in consultation with the Director of the National Security Agency, that provides options, timelines and required funding by the Armed Forces or a component of the Department, for the adoption of next generation encryption into existing and future systems.

(c) FORM.—The report under subsection (a) may be submitted in classified form.

(d) BRIEFING.—Not later than 30 days after the date on which the Secretary submits the report under subsection (a), the Chief Information Officer of the Department and the Director of the National Security Agency shall jointly provide to the appropriate congressional committees a briefing on the report.

(e) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committee on Armed Services, the Committee on Appropriations, and the Permanent Select Committee on Intelligence of the House of Representatives; and

(2) the Committee on Armed Services, the Committee on Appropriations, and the Select Committee on Intelligence of the Senate.

SEC. 716. REVIEW OF NATIONAL SECURITY AGENCY AND UNITED STATES CYBER COMMAND.

(a) REVIEW REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Inspectors General of the National Security Agency, Intelligence Community, and Department of Defense shall jointly complete a review of the National Security Agency and the United States Cyber Command.

(b) ELEMENTS.—The review required by subsection (a) shall include assessment of the following:

(1) Whether and what resources, authorities, activities, missions, facilities, and personnel are appropriately being delineated and used to conduct the intelligence and cybersecurity missions at the National Security Agency as well as the cyber offense and defense missions of the United States Cyber Command.

(2) The extent to which current resource-sharing arrangements between the National Security Agency and the United States Cyber Command lead to conflicts of interest in directing intelligence collec-

tion in support of United States Cyber Command missions rather than foreign intelligence collection.

(3) The intelligence analysis and production conducted by the United States Cyber Command using National Security Agency authorities, with a focus on analytic integrity and intelligence oversight to ensure proper analysis is informing mission operations.

(4) The number of personnel detailed from the National Security Agency to the United States Cyber Command, including from which offices such personnel have been detailed, and an assessment of the mission impact on the sponsoring office.

(c) REPORT AND BRIEF.—Not later than 180 days after the date of the enactment of this Act, the Inspectors General of the National Security Agency, Intelligence Community, and Department of Defense shall jointly submit to the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) a report and provide such committees a briefing on the findings of the inspectors general with respect to the review completed under subsection (a).



From	'(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>
To	"O'Donnell, Sean W., HON, OIG DoD" <(b) (6) @DODIG.MIL>
Cc	"Blair, Daniel R., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "Stebbins, Steven A., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, "FitzHarris, Leo J., SES, OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>, '(b) (6) , OIG DoD" <(b) (6) @DODIG.MIL>
Subject	WARs for October 16
Date	Fri, 16 Oct 2020 17:58:32 +0000
Message-Id	<0775b4cd08a54b52a1660b2be5769934@DODIG.MIL>

Mr. O'Donnell and All,
Attached are the WARs for this week. Chief, your WAR book is heading towards your office in-box soon. Have a good weekend all

.....

Attachment Name : AI WAR 10162020.pdf

.....

Attachment Name : AUDIT WAR 10162020.pdf

.....

Attachment Name : EEO WAR 10162020.docx

.....

Attachment Name : EVAL WAR 10162020.pdf

.....

Attachment Name : INV WAR 10162020.pdf

.....

Attachment Name : MST WAR 10162020.pdf

.....

Attachment Name : OCO WAR 10162020.pdf

.....

Attachment Name : OGC WAR 10162020.pdf

.....

Attachment Name : OLAC WAR 10162020.pdf

.....

Attachment Name : OPR WAR 10162020.pdf

~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

INFO MEMO

October 16, 2020

FOR: ACTING INSPECTOR GENERAL

FROM: Michael J. Roark, Deputy Inspector General for Evaluations

SUBJECT: Weekly Activity Report for October 2 – 15, 2020

Program, COCOM, & OCO Operations (Carolyn Hantz)

1. **Program Evaluations I** ((b) (6))
   a. **Draft Report:** (b) (5)
   b. **Fieldwork:** (b) (5)
   c. **Planning:** (b) (5)
   d. **Planning:** (b) (5)
   e. **Planning:** (b) (5)

2. **Program Evaluations II** ((b) (6))
   a. **Draft Report:** (b) (5)
   b. **Planning:** (b) (5)
   c. **Planning:** (b) (5)

3. **COCOMs ((b) (6))**
   a. **Draft Report:** (b) (5) [redacted]
   b. **Draft Report:** [redacted]
   c. **Planning:** (b) (5) [redacted]

4. **OCO ((b) (6))**
   a. **Draft Report:** (b) (5) [redacted]
   b. **Draft Report:** (b) (5) [redacted]
   c. **Draft Report:** (b) (5) [redacted]
   d. **Draft Report:** (b) (5) [redacted]
   e. **Planning:** (b) (5) [redacted]
   f. **Planning:** (b) (5) [redacted]

Space, Intelligence, Engineering, and Oversight (Randy Stone)

5. **Space, Missile, and Nuclear ((b) (6))**
   a. **Draft Report:** (b) (5) [redacted].
   b. **Draft Report:** (b) (5) [redacted].
   c. **Fieldwork:** (b) (5) [redacted]
   d. **Fieldwork:** (b) (5) [redacted]
   e. **Fieldwork:** (b) (5) [redacted]
   f. **Planning:** (b) (5) [redacted].

6. **Research and Engineering ((b) (6))**
   a. **Draft Report:** (b) (5) [redacted]
   b. **Draft Report:** (b) (5) [redacted]
   c. **Fieldwork:** (b) (5) [redacted]

(b) (5)

d. **Fieldwork:** (b) (5)

7. **Intelligence (** (b) (6) **)**

a. **Final Report:** (b) (5)

b. **Draft Report:** (b) (5)

c. **Draft Report:** (b) (5)

d. **Draft Report:** (b) (5)

e. **Fieldwork:** (b) (5)

f. **Fieldwork:** (b) (5)

g. **Fieldwork:** (b) (5)

h. **Planning:** (b) (5)

i. **Planning:** (b) (5) [redacted]

j. **Research:** (b) (5) [redacted]

8. **Sensitive Activities** (b) (6) [redacted])

a. **Draft Report:** (b) (5) [redacted]

b. **Fieldwork:** (b) (5) [redacted]

c. **Fieldwork:** (b) (5) [redacted]

d. **Planning:** (b) (5) [redacted]

9. **Audit Oversight** (b) (6) [redacted])

a. **Draft Report:** (b) (5) [redacted]

b. **Draft Report:** (b) (5) [redacted]

c. **Draft Report:** (b) (5) [redacted]

d. **Discussion Draft:** (b) (5) [redacted]

e. **Fieldwork:** (b) (5) [redacted]

f. **Fieldwork:** (b) (5) [redacted]

g. **Fieldwork:** (b) (5) [redacted]

h. **Fieldwork:** (b) (5) [redacted]

i. **Fieldwork:** (b) (5) [redacted]

j. **Planning:** (b) (5) [redacted]

k. **Planning:** (b) (5) [redacted]

l. **Planning:** (b) (5) [redacted]

10. Investigative Oversight ((b) (6) [redacted] **)**

a. **Fieldwork:** (b) (5) [redacted]

b. **Fieldwork:** (b) (5) [redacted]

c. **Planning:** (b) (5) [redacted]

d. **Planning:** [redacted].

Other Reporting

11. **Significant Activities and Events.**
    a. Mr. Stone, [redacted] met with [redacted] on October 15, 2020, to discuss Unidentified Aerial Phenomena (UAP).
    b. [redacted]
    c. [redacted]

12. **Component Head Priorities for Upcoming Week**
    a. [redacted]
    b. [redacted]
    c. [redacted].

13. **PRAC/COVID-19 related OIG oversight and activities**
    a. [redacted]

14. **Personnel Actions:**

(b) (5), (b) (6)

[redacted]

Submitted by (b) (6) [redacted]