

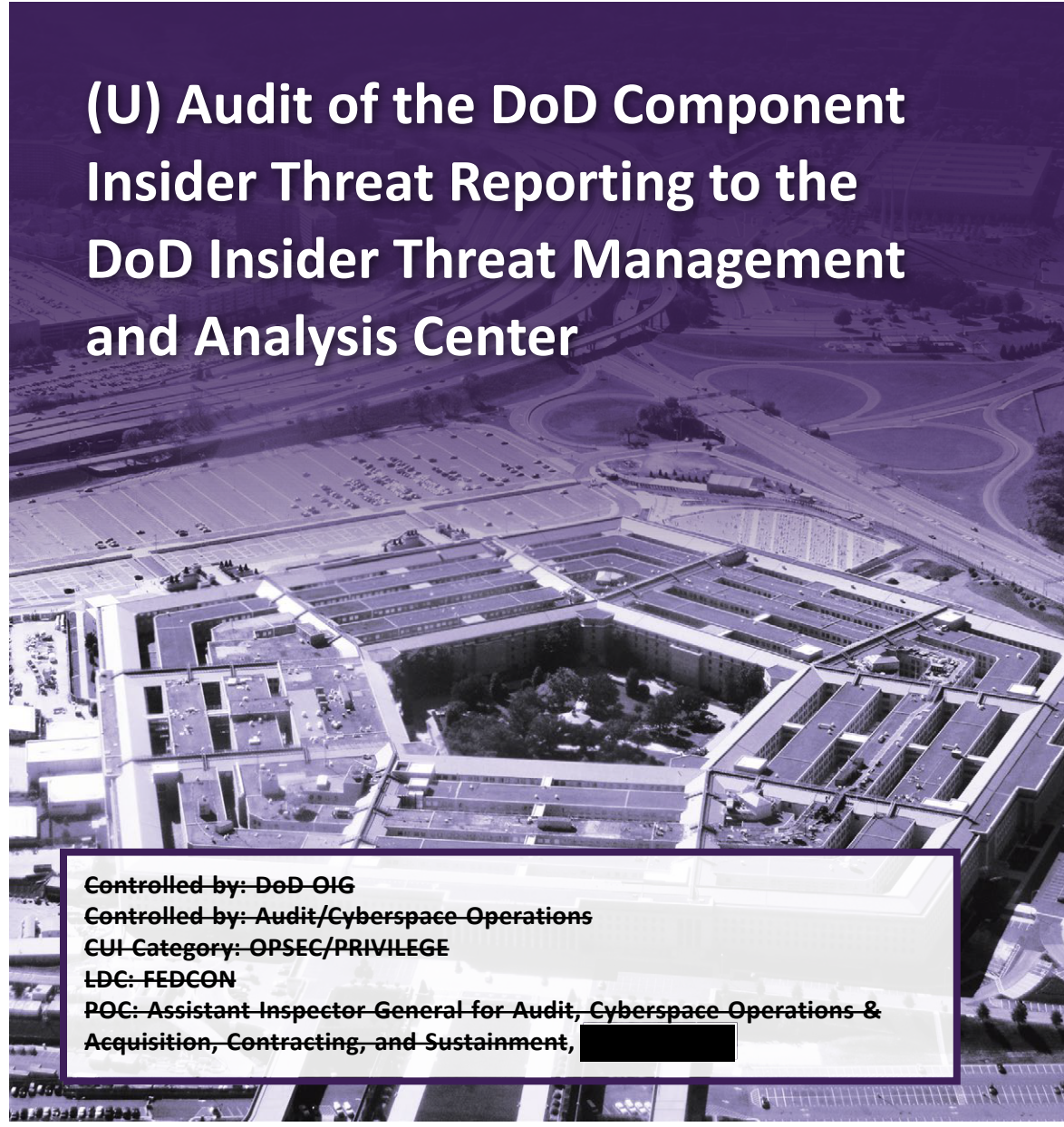


CUI

# INSPECTOR GENERAL

*U.S. Department of Defense*

SEPTEMBER 28, 2022



## (U) Audit of the DoD Component Insider Threat Reporting to the DoD Insider Threat Management and Analysis Center

Controlled by: DoD-OIG

Controlled by: Audit/Cyberspace Operations

CUI-Category: OPSEC/PRIVILEGE

LDC: FEDCON

POC: Assistant Inspector General for Audit, Cyberspace Operations & Acquisition, Contracting, and Sustainment, [REDACTED]

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

CUI





CUI

# (U) Results in Brief

## *(U) Audit of the DoD Component Insider Threat Reporting to the DoD Insider Threat Management and Analysis Center*

September 28, 2022

### (U) Objective

(U) The objective of this audit was to determine whether DoD Components reported insider threat incidents to the DoD Insider Threat Management and Analysis Center (DITMAC) in accordance with DoD guidance.

### (U) Background

(U) DoD Directive 5205.16 defines a DoD insider as any person (DoD personnel, contractors, and other non-DoD individuals) to whom the DoD has, or once had, granted eligibility for access to classified information or to hold a sensitive position. The Directive defines an insider threat as a threat that insiders pose to the DoD and Federal Government installations, facilities, personnel, missions, and resources, that can result in damage to the United States through espionage, terrorism, and unauthorized disclosure of national security information. The FY 2017 National Defense Authorization Act revised the definition of a DoD insider (also known as a covered person) to include any person who has, or once had, authorized access to DoD information, facilities, networks, or other resources. According to DoD officials, DoD Directive 5205.16 is being updated to reflect the revised definition of a DoD insider.

(U) DoD insiders have caused high-profile disclosures and breaches of data critical to national security. For example, since 2001, some of the most noted disclosures were

### (U) Background (cont'd)

(U) made by former National Security Agency (NSA) contractors Edward Snowden and Harold Martin. DoD insiders were also responsible for the mass shootings at Fort Hood in 2009 and at the Washington Navy Yard in 2013.

(U) After the Navy Yard shooting in 2013, the Secretary of Defense commissioned independent panels to review gaps and deficiencies in DoD security programs, policies, and procedures. In response to recommendations made in the panel reports, the Secretary of Defense approved the formation of DITMAC to provide a centralized capability to manage and analyze DoD insider threat data. DITMAC helps prevent, deter, detect, and mitigate the potential threat that DoD insiders may pose to the United States.

(U) In 2016, the Under Secretary of Defense for Intelligence and Security (USD[I&S]), who serves as the DoD senior official responsible for overseeing the DoD Insider Threat Program, established DITMAC within the Defense Counterintelligence and Security Agency. The USD(I&S) also directed that all DoD Components report insider threats to DITMAC. DoD Components are required to report to DITMAC through their Component's insider threat analysis center, known as an Insider Threat Hub. DoD military, civilian, and contractor personnel are required to report any incidents that involve a covered person (DoD insider) and meet one or more of the 13 reporting thresholds established by DITMAC. Examples of reportable incidents involve sexual assault, violent acts, questionable allegiance to the United States, unauthorized disclosure of classified information, and terrorism. DITMAC receives insider threat incidents from the Hubs electronically through the DITMAC System of Systems or e-mail.

### (U) Finding

(U) The Army, Navy, Marine Corps, Defense Logistics Agency, and Defense Health Agency Component Hubs did not consistently report to DITMAC insider threat incidents that involved a covered person and met one or more of the reporting

CUI



# (U) Results in Brief

## *(U) Audit of the DoD Component Insider Threat Reporting to the DoD Insider Threat Management and Analysis Center*

### **(U) Finding (cont'd)**

(U) thresholds. Specifically, of the 215 insider threat incidents we reviewed from those Hubs, 200 incidents involved a covered person and met one or more of the thresholds. Of those 200 incidents, 115 were reported to DITMAC, but the other 85 were not. Furthermore, of the 115 insider threat incidents that were reported to DITMAC, the time it took the Hubs to report the incidents ranged from 1 day to over 2 years.

(U) The inconsistent reporting to DITMAC occurred because the USD(I&S) did not:

- (U) develop an oversight program to periodically verify that the Hubs reported insider threat incidents that involved a covered person and met one or more of the reporting thresholds; and
- (U) establish timelines for reporting insider threat incidents to DITMAC.

(CUI) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) Insider threat incidents have resulted in harm to the United States and the DoD through espionage, terrorism, unauthorized disclosure of national security information, and the loss or degradation of DoD resources and capabilities. Unless the DoD Component Hubs consistently report insider threat incidents to

(U) DITMAC as required, DITMAC cannot fully accomplish its mission to provide the DoD with a centralized capability to identify, mitigate, and counter insider threats and reduce the harm to the United States and the DoD by malicious insiders.

### **(U) Recommendations**

(U) We recommend that the USD(I&S) implement a process for assessing DoD Component compliance with insider threat reporting requirements, develop timelines for DoD Components to report insider threat incidents to DITMAC, and submit the FY 2021 annual report on the DoD Insider Threat Program to the Secretary of Defense as required.

(U) We also recommend that the Secretary of the Army, the Secretary of the Navy, and the Defense Health Agency Director require that their Hub Directors review the insider threat incidents that we determined should have been reported to DITMAC and report those incidents as required. Lastly, we recommend that the NRO Director, USCYBERCOM Commander, and the NSA/Central Security Service Director require that their Hub Directors review the insider threat incidents received since the establishment of their Hubs or the 2016 DoD Component reporting requirement was initiated and report any of the incidents that involve a covered person and meet one or more of the reporting thresholds.

### **(U) Management Comments and Our Response**

(U) The DoD Counter-Insider Threat Deputy Director, responding for the USD(I&S), agreed to implement a process for assessing DoD Component compliance with



# (U) Results in Brief

## *(U) Audit of the DoD Component Insider Threat Reporting to the DoD Insider Threat Management and Analysis Center*

### *(U) Comments (cont'd)*

(U) insider threat reporting requirements, develop timelines for DoD Components to report insider threat incidents to DITMAC, and submit the DoD Insider Threat Program annual report to the Secretary of Defense.

~~(CUI)~~ The Under Secretary of the Army, responding for the Secretary of the Army, and the Deputy Under Secretary of the Navy for Intelligence and Security, responding for the Secretary of the Navy, agreed to report the incidents identified in this report to DITMAC. In addition, the USCYBERCOM Chief of Staff, responding for the USCYBERCOM Commander, agreed [REDACTED]

~~(CUI)~~ The NRO Director and the NSA Chief of Staff for Workforce Support Activities, responding for the NSA/Central Security Service Director, disagreed [REDACTED]

~~(CUI)~~ We disagree [REDACTED]

[REDACTED] The FY 2017 National Defense Authorization Act revised the definition of a DoD insider (covered person) to include any person who has, or once had, authorized access to DoD information, facilities, networks, or other resources. [REDACTED]

~~(CUI)~~ [REDACTED]

[REDACTED] Therefore, the recommendations to NRO and NSA are unresolved, and we request that the NRO Director and the NSA/Central Security Service Director provide comments on the final report.

(U) The Defense Health Agency Director did not provide comments on the draft report; therefore, we request that the Defense Health Agency provide comments on the final report.

(U) Please see the Recommendations Table on the next page for the status of recommendations.

***(U) Recommendations Table***

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
(U) Secretary of the Army	None	None	1
(U) Secretary of the Navy	None	None	2
(U) Under Secretary of Defense for Intelligence and Security	None	3.a., 3.b., and 3.c.	None
(U) Commander, U.S. Cyber Command	None	4	None
(U) Director, National Reconnaissance Office	5	None	None
(U) Director, Defense Healthy Agency	6	None	None
(U) Director, National Security Agency/ Central Security Service	7	None	None

(U) Please provide Management Comments by October 28, 2022.

**(U) Note:** The following categories are used to describe agency management’s comments to individual recommendations.

- **(U) Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **(U) Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **(U) Closed** – DoD OIG verified that the agreed upon corrective actions were implemented.



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

September 28, 2022

(U) MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE  
AND SECURITY,  
COMMANDER, U.S. CYBER COMMAND  
DIRECTOR, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE  
DIRECTOR, DEFENSE HEALTH AGENCY  
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE  
AUDITOR GENERAL, DEPARTMENT OF THE ARMY  
AUDITOR GENERAL, DEPARTMENT OF THE NAVY

(U) SUBJECT: Audit of the DoD Component Insider Threat Reporting to the DoD Insider  
Threat Management and Analysis Center (Report No. DODIG-2022-141)

(U) This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) This report contains three recommendations that are considered unresolved because management officials did not fully address or did not respond to the recommendations. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations will remain unresolved until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, the recommendations will be closed.

(U) This report contains four recommendations that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, the recommendations will be closed.

(U) This report contains two recommendations that are considered closed as discussed in the Recommendations, Management Comments, and Our Response section of this report. Those recommendations do not require further action.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, within 30 days please provide us your comments concerning specific actions in process or alternative corrective actions proposed on the recommendations. For the resolved recommendations, within 90 days please provide us documentation showing that the agreed-upon action has been completed. Your response should be sent as a PDF file

(U) to [audcso@dodig.mil](mailto:audcso@dodig.mil) if unclassified or [rfunet@dodig.smil.mil](mailto:rfunet@dodig.smil.mil) if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

(U) We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact me at [REDACTED]



Carol N. Gorman

Assistant Inspector General for Audit  
Cyberspace Operations & Acquisition,  
Contracting, and Sustainment



# (U) Contents

---

## (U) Introduction

(U) Objective..... 1

(U) Background..... 1

(U) Review of Internal Controls..... 6

## (U) Finding. DoD Component Hubs Did Not Consistently Report Insider Threat Incidents to DITMAC

(U) DoD Component Hubs Did Not Follow Insider Threat Reporting Guidance..... 8

(U) USD(I&S) Did Not Provide Oversight of the DoD Insider Threat Program..... 14

(U) USD(I&S) Did Not Establish Timelines for Reporting Insider Threat Incidents to DITMAC..... 15

(U) [REDACTED]..... 15

(U) The DoD Is at Risk of Not Identifying or Mitigating Critical Insider Threats..... 16

(U) Other Matters of Interest..... 17

(U) Recommendations, Management Comments, and Our Response..... 18

## (U) Appendixes

(U) Appendix A. Scope and Methodology..... 25

    (U) Use of Computer-Processed Data..... 26

    (U) Use of Technical Assistance..... 27

    (U) Prior Coverage..... 27

(U) Appendix B. DoD Insider Threat Incidents..... 28

(U) Appendix C. DITMAC Reporting Thresholds..... 30

## (U) Management Comments

(U) Department of the Army..... 33

(U) Department of the Navy..... 34

(U) Under Secretary of Defense for Intelligence and Security..... 36

(U) DoD Insider Threat Management and Analysis Center..... 38

## **(U) Contents (cont'd)**

---

(U) U.S. Cyber Command.....	39
(U) National Reconnaissance Office .....	40
(U) National Security Agency.....	42
<b>(U) Acronyms and Abbreviations.....</b>	<b>43</b>

# (U) Introduction

## (U) Objective

(U) The objective of this audit was to determine whether DoD Components reported insider threat incidents to the DoD Insider Threat Management and Analysis Center (DITMAC) in accordance with DoD guidance. See Appendix A for a discussion of the scope, methodology, and prior coverage related to the objective.

## (U) Background

(U) DoD Directive 5205.16 defines a DoD insider as any person (DoD personnel, contractors, and individuals from other non-DoD entities) to whom the DoD has or had granted eligibility for access to classified information or to hold a sensitive position.<sup>1</sup> The Directive defines an insider threat as a threat that DoD insiders pose to DoD and U.S. Government installations, facilities, personnel, missions, and resources. This threat can include damage to the United States through espionage, terrorism, and unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

*(U) The Directive defines an insider threat as a threat that DoD insiders pose to DoD and U.S. Government installations, facilities, personnel, missions, and resources.*

(U) The FY 2017 National Defense Authorization Act revised the definition of a DoD insider to include any person who has, or once had, authorized access to DoD information, facilities, networks, or other resources.<sup>2</sup> According to DoD officials, DoD Directive 5205.16 is being updated to reflect the revised definition of a DoD insider.

(U) DoD insiders with malicious intent have been responsible for high-profile disclosures and breaches of data critical to national security. For example, since 2001, former Defense Intelligence Agency senior analyst Ana Montes, Army Intelligence Analyst Bradley Manning (now Chelsea Manning), National Security Agency (NSA) contractors Edward Snowden and Harold Martin, and U.S. Navy nuclear engineer Jonathan Toebbe and his wife all made disclosures that negatively impacted the DoD. DoD insiders were also responsible for the mass shootings at Fort Hood, Texas, in 2009 and at the Washington Navy Yard in 2013. For additional information on those incidents, see Appendix B.

<sup>1</sup> (U) DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, (Incorporating Change 2, August 28, 2017). Sensitive positions do not require access to classified information but do require individuals to perform duties related to national security.  
<sup>2</sup> (U) Public Law 114-328, "National Defense Authorization Act for Fiscal Year 2017," section 951, December 23, 2016.

## ***(U) Federal and DoD Insider Threat Guidance***

(U) In October 2011, the President issued Executive Order 13587, requiring all Executive Branch departments and agencies to implement an insider threat detection and prevention program.<sup>3</sup> The Executive Order also requires that the National Insider Threat Task Force (NITTF) develop and issue guidance and minimum standards for implementing an insider threat program for Executive Branch departments and agencies.

(U) In November 2012, the President issued a Presidential Memorandum that identifies the National Insider Threat Policy and minimum standards (NITTF minimum standards).<sup>4</sup> To meet the minimum standards, Executive Branch departments and agencies were required to establish insider threat policy, provide training for personnel to conduct insider threat related activities, ensure timely access to insider threat related information, and monitor user activity on information systems and networks. The NITTF minimum standards also require that Executive Branch departments and agencies designate a senior official responsible for the implementation and management of their respective Insider Threat Program.

(U) In September 2013, the Deputy Secretary of Defense designated the Under Secretary of Defense for Intelligence and Security (USD[I&S]) as the DoD senior official responsible for DoD's Insider Threat Program. In September 2014, the Deputy Secretary of Defense issued DoD Directive 5205.16, which requires that the USD(I&S) develop and maintain a DoD Insider Threat Program to comply with the NITTF minimum standards. The Directive states that the purpose of the Insider Threat Program is to gather, assess, and respond to insider threat information derived from counterintelligence, security, cybersecurity, civilian and military personnel management, workplace violence, antiterrorism risk management, law enforcement, user activity on DoD information networks, and other sources as necessary and appropriate to identify, mitigate, and counter insider threats.

*(U) In September 2013, the Deputy Secretary of Defense designated the Under Secretary of Defense for Intelligence and Security (USD[I&S]) as the DoD senior official responsible for DoD's Insider Threat Program.*

<sup>3</sup> (U) Presidential Executive Order No. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011.

<sup>4</sup> (U) Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012.

**(U) DITMAC**

(U) After the Navy Yard shooting in 2013, the Secretary of Defense commissioned independent panels to review gaps and deficiencies in DoD security programs, policies, and procedures.<sup>5</sup> In response to recommendations made in the panel reports, the Secretary approved the formation of DITMAC to provide a centralized capability to manage and analyze DoD insider threat data. DITMAC helps prevent, deter, detect, and mitigate the potential threat that DoD insiders may pose to the United States. In 2014, the USD(I&S), who serves as the DoD senior official responsible for overseeing the DoD Insider Threat Program, established DITMAC within the Defense Counterintelligence and Security Agency (DCSA).<sup>6</sup> DoD Instruction 5205.83 states that DITMAC will:

*(U) The Secretary approved the formation of DITMAC to provide a centralized capability to manage and analyze DoD insider threat data. DITMAC helps prevent, deter, detect, and mitigate the potential threat that DoD insiders may pose to the United States.*

- (U) oversee the mitigation of DoD insider threats;
- (U) assess enterprise-level (DoD-wide) insider threat risks, refer recommendations for action to the Office of the USD(I&S) (OUSD[I&S]), coordinate responses, and oversee resolution of identified insider threat concerns;
- (U) develop DoD-wide risk criteria (thresholds) to facilitate component reporting of insider threat information and assessing the effectiveness of actions taken by DoD Components to address, mitigate, or resolve insider threats;
- (U) support the OUSD(I&S) in establishing standards to ensure that the DoD Insider Threat Program complies with applicable statutes, executive orders, and other Federal and DoD guidance that specifies insider threat program requirements;
- (U) provide a single repository for information related to DoD insider threats; and
- (U) promote collaboration and sharing of insider threat information among DoD Components.<sup>7</sup>

<sup>5</sup> (U) USD(I&S) Report, “DoD Internal Review of the Washington Navy Yard Shooting: A Report to the Secretary of Defense,” November 20, 2013.

<sup>6</sup> (U) OUSD(I&S) Memorandum for Director, Defense Security Service, “Incubation of the DoD Insider Threat Management Analysis Center,” December 12, 2014. The Defense Security Service is now called the Defense Counterintelligence and Security Agency (DCSA).

<sup>7</sup> (U) DoD Instruction 5205.83, “DoD Insider Threat Management, and Analysis Center (DITMAC),” March 30, 2017, (Incorporating Change 1, October 29, 2020).

(U) In addition, DoD Directive 5205.16 requires DITMAC to develop reporting criteria (thresholds) for DoD Components to report insider threats, which we will refer to as incidents for the purposes of this report. In 2016, DITMAC issued 13 reporting thresholds (DITMAC Reporting Thresholds) as a guide for the DoD Components to use when determining whether an insider threat incident merits DoD-wide awareness and reporting to DITMAC.<sup>8</sup> For example, the DITMAC Reporting Thresholds include guidance on reporting incidents to DITMAC involving sexual assault or violent acts, concerning behavior, allegiance to the United States, unauthorized disclosure, and terrorism. See Appendix C for a list and description of the 13 reporting thresholds.

### ***(U) DoD Insider Threat Reporting Process***

(U) In December 2016, the USD(I&S) directed all DoD Components to submit information on insider threat incidents that meet one or more of the 13 reporting thresholds to DITMAC.<sup>9</sup> DoD military personnel, civilian employees, and contractor personnel are required to report potential insider threats or incidents to their supervisor or local security office, who in turn must share the information with their component's insider threat analysis center (known as a Hub).<sup>10</sup> The Hubs treat all reported incidents as a potential insider threat until they have verified whether the threat or incident meets one or more of the DITMAC Reporting Thresholds.

*(U) In December 2016, the USD(I&S) directed all DoD Components to submit information on insider threat incidents that meet one or more of the 13 reporting thresholds to DITMAC.*

(U) The DITMAC Reporting Thresholds require Hub officials to report incidents involving a DoD insider or a "covered person." DITMAC defines a covered person as an individual who meets the DoD Directive 5205.16 definition of a DoD insider, which is currently being updated. Examples of a DoD covered person include:

- (U) active and reserve military personnel and their family members, with active Uniformed Services identification cards;
- (U) civilian employees;
- (U) contractors;
- (U) individuals from other non-DoD entities, such as federal, state, local, tribal, and private sector entities affiliated or working with the DoD and granted access to classified information; or

<sup>8</sup> (U) USD(I&S), "DoD Insider Threat Management & Analysis Center Reporting Thresholds: Desk Reference Guide," December 2016.

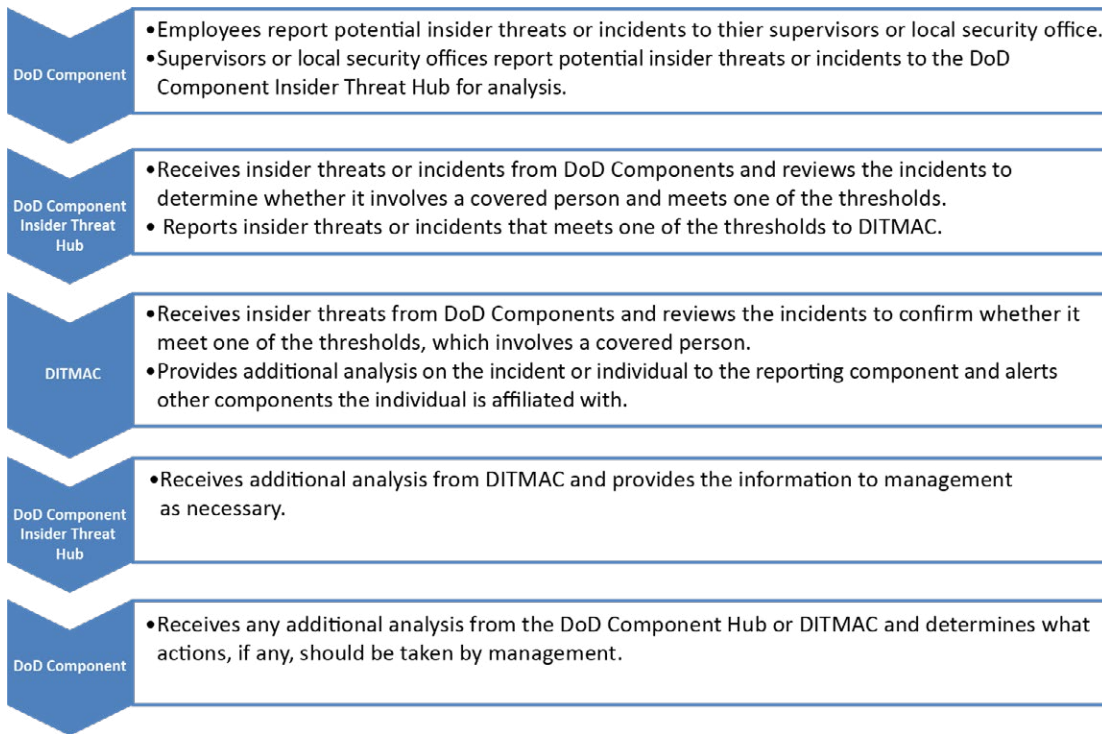
<sup>9</sup> (U) The USD(I&S) memorandum, "Reporting Information to the Department of the Defense Insider Threat Management and Analysis Center," December 29, 2016.

<sup>10</sup> (U) The Center for Development of Security Excellence, Insider Threat Job Aid, "Insider Threat Reporting." For the purpose of this report, we are referring to the DoD Component's insider threat analysis center as Hubs.

- (U) individuals with an active identification card, pass, or credential from a DoD organization—such as a DoD common access card—used as proof of identification to gain physical or logical access to a DoD facility, network, system, or program.<sup>11</sup>

(U) If the Hub determines that an incident involving a covered person meets one or more of the 13 reporting thresholds, officials must report the incident to DITMAC. DITMAC verifies whether the Hub reported insider threat incident involves a covered person and meets one or more of the 13 reporting thresholds. DITMAC provides any additional analysis on the incident or the individual involved to the reporting component and alerts any other DoD Components affiliated with the individual. See Figure 1 below for a flowchart of the DoD insider threat reporting process.

(U) Figure 1. Flowchart of DoD Insider Threat Reporting Process



(U) Source: The DoD OIG.

(U) DITMAC receives insider threat incidents from the DoD Component Hubs electronically through a case management system—the DITMAC System of Systems (DSoS)—or e-mail when DSoS cannot be used.<sup>12</sup> The DoD Component Hubs use DSoS as the primary tool to capture, consolidate, store, and manage insider threat data. The Hubs can access DSoS, a web portal application, on the

<sup>11</sup> (U) The Office of the Secretary of Defense System of Record Notice, “DITMAC and DoD Component Insider Threat Records System,” March 22, 2019.

<sup>12</sup> (U) According to DITMAC officials, DITMAC created a form that could be sent over unclassified, SIPR, or JWICS e-mail, depending on the classification of the incident information.

(U) Secret Internet Protocol Router Network to report insider threat incidents to DITMAC.<sup>13</sup> In addition, according to DoD Officials' DSoS was available on the Joint Worldwide Intelligence Communications System (JWICS) for DoD Component use in January 2021.

~~(CUI)~~ To determine whether Hubs properly reported insider threat incidents to DITMAC, we selected seven DoD Component Hubs for review—the Army, Navy, Marine Corps, Defense Logistics Agency (DLA), Defense Health Agency (DHA), National Reconnaissance Office (NRO), and U.S. Cyber Command (USCYBERCOM).<sup>14</sup> For the Army, Navy, Marine Corps, DLA, and DHA Hubs, we nonstatistically selected potential insider threats or incidents reported to DITMAC to determine whether Hub officials reported incidents involving a covered person that met one or more of the thresholds as required by DoD guidance. [REDACTED]

## (U) Review of Internal Controls

(U) DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.<sup>15</sup> We identified that the DoD Components Hubs were not consistently reporting insider threat incidents to DITMAC in accordance with DoD guidance. We will provide a copy of the final report to the senior official responsible for internal controls in the USD(I&S), DCSA, and the DoD Components.

<sup>13</sup> (U) Hubs share information with DITMAC about insider threats, including analysis, notes, any related or linked insider threat incidents or files, and mediation actions.

<sup>14</sup> (U) Although the Department of the Navy considers itself as one insider threat hub, we observed the Navy running two separate insider threat Hubs and reporting incidents separately to DITMAC. Therefore, we are treating the Navy and the Marine Corps Hubs as separate Hubs for the purposes of this report.

<sup>15</sup> (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, (Incorporating Change 1, June 30, 2020).



## (U) Finding

### (U) DoD Component Hubs Did Not Consistently Report Insider Threat Incidents to DITMAC

(U) The Army, Navy, Marine Corps, DLA, and DHA Component Hubs did not consistently report to DITMAC insider threat incidents that involved a covered person and met one or more of the reporting thresholds. Specifically, of the 215 insider threat incidents we reviewed from those Hubs, 200 incidents involved a covered person and met one or more of the thresholds. Of those 200 incidents, 115 were reported to DITMAC, but the other 85 were not. Furthermore, of the 115 insider threat incidents that were reported to DITMAC, the time it took the Hubs to report the incidents ranged from 1 day to over 2 years. The inconsistent reporting to DITMAC occurred because the USD(I&S) did not:

- (U) develop an oversight program to periodically verify that the Hubs reported insider threat incidents that involved a covered person and met one or more of the reporting thresholds; and
- (U) establish timelines for reporting insider threat incidents to DITMAC.

(CUI) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) Insider threat incidents have resulted in harm to the United States and the DoD through espionage, terrorism, unauthorized disclosure of national security information, and the loss or degradation of DoD resources and capabilities. Unless the DoD Component Hubs consistently report insider threat incidents to DITMAC as required, DITMAC cannot fully accomplish its mission to provide the DoD with a centralized capability to identify, mitigate, and counter insider threats and reduce the harm to the United States and the DoD by malicious insiders.

## (U) DoD Component Hubs Did Not Follow Insider Threat Reporting Guidance

(U) The Army, Navy, Marine Corps, DLA, and DHA Component Hubs did not report all insider threat incidents that involved a covered person and met one or more of the reporting thresholds to DITMAC, as required. To determine whether those Hubs appropriately reported insider threat incidents to DITMAC, we selected 215 incidents consisting of 143 reported and 72 that were not. Of the 215 insider threat incidents reviewed from those Hubs, 200 incidents involved a covered person and met one or more of the thresholds. Of those 200 incidents, 115 were reported to DITMAC, but the other 85 were not as of March 2021. Table 1 contains the incident review results by Hub.

*(U) Of those 200 incidents, 115 were reported to DITMAC, but the other 85 were not as of March 2021.*

*(U) Table 1. Results of Incident Review by Hub (as of March 2021)*

(U) DoD Component Hub	(U) Incidents Reviewed	(U) Incidents That Met One or More Thresholds	(U) Incidents Reported to DITMAC	(U) Incidents Not Reported to DITMAC But Should Have Been
(U) Army	58	54	45	9
(U) Navy	68	67	41	26
(U) Marine Corps	30	30	7	23
(U) DLA	30	25	13	12
(U) DHA	29	24	9	15
<b>(U) Total</b>	<b>215</b>	<b>200</b>	<b>115</b>	<b>85</b>

(U) Source: The DoD OIG.

(U) Furthermore, of the 115 insider threat incidents that the Army, Navy, Marine Corps, DLA, and DHA reported to DITMAC, the time it took the Hubs to report the incidents ranged from 1 day to over 2 years. Table 2 lists the reporting timeframes by Hub.

*(U) Of the 115 insider threat incidents that the Army, Navy, Marine Corps, DLA, and DHA reported to DITMAC, the time it took the Hubs to report the incidents ranged from 1 day to over 2 years.*

(U) Table 2. Hub Reporting Timeframes

(U) DoD Component Hub	(U) Incidents Reported < 30 Days	(U) Incidents Reported 31 - 180 Days	(U) Incidents Reported 181 - 365 Days	(U) Incidents Reported 1-2 years	(U) Incidents Reported > 2 years	(U) Total
(U) Army	4	8	16	10	7	45
(U) Navy	3	11	9	8	1	32 <sup>1</sup>
(U) Marine Corps	6	1	–	–	–	7
(U) DLA	6	7	–	–	–	13
(U) DHA	5	–	–	–	–	5 <sup>2</sup>
(U) Total	24	27	25	18	8	102

<sup>1</sup> (U) The Navy Hub did not track when the Hub received nine incidents; as a result, the Navy could not provide the reporting timeframes for those incidents..

<sup>2</sup> (U) The DHA Hub did not track when the Hub received four incidents; as a result, the DHA could not provide the reporting timeframes for those incidents.

(U) Source: The DoD OIG.

### (U) Army Hub Reporting

(U) Of the 58 Army Hub incidents reviewed, we determined that 54 incidents involved a covered person and met one or more of the DITMAC Reporting Thresholds. As of March 2021, the Army Hub reported 45 of those incidents to DITMAC but did not report the other 9. For the 45 incidents reported to DITMAC, the Army Hub reported 4 incidents within 30 days of receiving the incident but took over 1 year to report 10 incidents and over 2 years to report 7 incidents.

(U) The nine insider threat incidents not reported to DITMAC involved aggravated assault, domestic violence, and domestic battery. For example, one incident involved a covered person who was charged with domestic violence, third-degree assault, and driving under the influence of alcohol. The incident met DITMAC Reporting Threshold Number 6–Criminal Conduct, which requires the Hubs to report:

*(U) The nine insider threat incidents not reported to DITMAC involved aggravated assault, domestic violence, and domestic battery.*

(U) The investigation, arrest, or apprehension by a federal, state, or local law enforcement agency, or the conviction, indictment, or charging by a federal, state or local jurisdiction of any covered person involving: the loss of life; actual or suspected acts of violence or threats of violence (including sexual assault); the illegal possession or transfer of weapons of mass destruction; or any criminal offenses involving the use of weapons or explosives.

(U) Army Hub officials stated that the incident was pending submission to DITMAC but was not a reporting priority because it was not high risk. However, Army Hub officials had labeled the incident as high risk within their insider threat tracker.

### ***(U) Navy Hub Reporting***

(U) Of the 68 Navy Hub incidents reviewed, we determined that 67 incidents involved a covered person and met one or more of the DITMAC Reporting Thresholds. As of March 2021, the Navy Hub reported 41 of those incidents to DITMAC but did not report the other 26. For the 41 incidents reported to DITMAC, the Navy Hub reported 3 incidents within 30 days of receiving the incident but took over 1 year to report 8 incidents and over 2 years to report one incident.

(U) The 26 insider threat incidents not reported to DITMAC involved murder, rape, kidnapping, aggravated assault, robbery, and soliciting sexual conduct with a minor. For example, one incident involved a covered person who was arrested

*... (U) The 26 insider threat incidents not reported to DITMAC involved murder, rape, kidnapping, aggravated assault, robbery, and soliciting sexual conduct with a minor.*

for several charges, including unlawful videotaping, dissemination of video or image with the intent to harass, and several counts of assault. This incident met DITMAC Reporting Threshold Number 6–Criminal Conduct. Navy Hub officials initially labeled the incident as “high risk” and reportable to DITMAC, but they subsequently decided not to report the incident because the charges were dismissed and the individual had not “demonstrated continued negative decisions, actions, or behaviors.” However, the threshold for criminal conduct does not make concessions for subsequent non-negative behavior or mention that reporting is not required if an individual’s charges are later dismissed; therefore, the incident should have been reported to DITMAC.

(U) Another example involved an individual who was charged with sexual assault, which also met DITMAC Reporting Threshold 6. Navy Hub officials stated that the incident was not reported because the individual separated from the Navy before the Hub received the incident. However, the Navy Hub should have reported this

(U) incident to DITMAC because the individual was a covered person at the time of incident and would be relevant if the individual attempted to return to the DoD in another status.

(U) After we completed our review, the Navy Hub reported the two incidents described above to DITMAC in May 2022 and June 2022, respectively. The Navy Hub also submitted another 20 unreported incidents to DITMAC between April 2021 and June 2022. The remaining 4 incidents have not been reported to DITMAC as of June 2022.

**(U) Marine Corps Hub Reporting**

(U) Of the 30 Marine Corps Hub incidents reviewed, we determined that 30 incidents involved a covered person and met one or more of the DITMAC Reporting Thresholds. As of March 2021, the Marine Corps Hub reported 7 of the incidents to DITMAC but did not report the other 23. For the seven incidents reported to DITMAC, the Marine Corps Hub reported six within 30 days and one in 57 days.

<p>(U) The 23 insider threat incidents not reported to DITMAC involved terroristic threats, use of a deadly weapon, assault, aggravated battery, and sexual exploitation of a minor. For example, one of those incidents involved a covered person who was part of a broader investigation into domestic terrorism and was arrested for attempting to illegally purchase a weapon. Similar to the previous Hub examples, this incident met DITMAC Reporting Threshold Number 6–Criminal Conduct.</p>	<p>⋮ <i>(U) The 23 insider threat incidents not reported to DITMAC involved terroristic threats, use of a deadly weapon, assault, aggravated battery, and sexual exploitation of a minor.</i></p>
--	---

(U) After we completed our review, Marine Corps Hub reported the incident described above in May 2021. The Marine Corps Hub also submitted another 17 unreported incidents to DITMAC between April 2021 and May 2022. The remaining 5 incidents have not been reported to DITMAC as of June 2022.

**(U) DLA Hub Reporting**

(U) Of the 30 DLA Hub incidents reviewed, 25 involved a covered person and met one or more of the DITMAC Reporting Thresholds. As of March 2021, the DLA Hub reported 13 of the incidents to DITMAC but did not report the other 12. For the 13 incidents reported to DITMAC, the DLA Hub reported 6 within 30 days, and the remaining 7 took up to 116 days.

(U) The 12 insider threat incidents that were not reported to DITMAC involved harassment, stalking, threatening to harm other DoD personnel with a weapon, and misuse of information technology systems. For example, one incident involved a covered person who had exhibited extreme personality and performance changes at

work, demonstrated hostility and anger towards DoD personnel, and wrote a letter to upper management idealizing Edward Snowden. This incident met DITMAC Reporting Threshold Number 4–Personal Conduct, which requires the Hubs to report:

(U) Information, in regard to a covered person, pertaining to deliberate omission, concealment, or falsification of relevant facts from any personnel security investigations, polygraph examinations (including counterintelligence scope and expanded screening scope polygraphs), or a pattern of behavior (two or more incidents closely related in time) that puts the individual’s judgment, trustworthiness, candor, honesty or willingness to comply with applicable laws and regulations into question.

(U) This incident also met DITMAC Reporting Threshold Number 5–Behavioral Considerations, which requires the Hubs to report:

(U) Information pertaining to a covered person who exhibits behaviors that cast doubts on their judgment, reliability, or trustworthiness. Such behaviors include, but are not limited to, emotionally unstable, irresponsible, dysfunctional, violent, paranoid, bizarre, anti-social, or aggressive behavior (see ‘Violence in the Federal Workplace: A Guide for Prevention and Response,’ for additional information about these behaviors of concern). This also includes information derived from User Activity Monitoring (UAM), human resources information, military and civilian performance evaluations, and reports of criminal or family law proceedings that indicate a person cleared by DoD is a threat to him or herself. Seeking mental health counselling is not by itself a reporting threshold.

(U) After we completed our review, the DLA Hub reported the incident described above to DITMAC in June 2022. The DLA Hub also submitted another 11 unreported incidents to DITMAC in June 2022. Because the DLA Hub reported all 12 incidents reviewed, we are not making a recommendation to DLA in this report.

*(U) The 12 insider threat incidents that were not reported to DITMAC involved harassment, stalking, threatening to harm other DoD personnel with a weapon, and misuse of information technology systems.*

**(U) DHA Hub Reporting**

(U) Of the 29 DHA Hub incidents reviewed, we determined that 24 incidents involved a covered person and met one or more of the DITMAC Reporting Thresholds. As of March 2021, the DHA Hub reported 9 of the incidents to DITMAC but did not report the other 15. For the nine incidents reported to DITMAC, the DHA Hub reported five incidents within 7 days; however, we could not determine the elapsed days for the remaining four because the Hub did not track the open date for those incidents.

*(U) The 15 insider threat incidents that were not reported to DITMAC involved the possession of an illegal substance, bringing an unauthorized visitor into a DoD facility, and expressing intent to harm oneself or others.*

(U) The 15 insider threat incidents that were not reported to DITMAC involved the possession of an illegal substance, bringing an unauthorized visitor into a DoD facility, and expressing intent to harm oneself or others. For example, one incident involved a covered person who brought an unauthorized visitor to their

workplace. The unauthorized visitor had a verbal exchange with a DHA employee, which left the employee feeling threatened. The DHA employee subsequently reported the incident to the police. This incident resulted in revoking the covered person’s badge access and the removal from their position. Similar to a previous Hub example, this incident met DITMAC Reporting Threshold Number 5–Behavioral Considerations. DHA Hub officials stated that this incident was not reported because the individual had resigned from their position. However, the DHA Hub should have reported this incident to DITMAC because the individual was a covered person at the time of incident and would be relevant if the individual attempted to return to the DoD in another status.

(U) Another example involved a covered person who was using their Government-issued equipment to send messages on social media that suggested a desire to harm themselves and others. This incident also met the DITMAC Reporting Threshold Number 5–Behavioral Considerations. DHA Hub officials stated that the incident was not reported to DITMAC because the individual sending the messages was not affiliated with the DHA and thus, the incident was referred to the individual’s command for action. However, the DITMAC Reporting Threshold guidance requires Hubs to report insider threat incidents involving a covered person to DITMAC and does not specify that the covered person must be affiliated with the Hub that received notification of the incident. Since this incident involved a covered person and met a reporting threshold, the DHA Hub should have reported the incident to DITMAC because the individual was still a possible threat to themselves and other DoD personnel.

*(U) Of the 85 unreported cases, the Navy, Marine Corps, and the DLA Hubs submitted 52 cases to DITMAC between April 2021 and June 2022, including all 12 unreported incidents from the DLA Hub.*

(U) Overall, we identified 85 insider threat incidents that the 5 Hubs should have reported to DITMAC but did not as of March 2021. Of the 85 unreported cases, the Navy, Marine Corps, and the DLA Hubs submitted 52 cases to DITMAC between April 2021 and June 2022, including all 12 unreported incidents

from the DLA Hub. Therefore, we recommend that the Secretary of the Army, the Secretary of the Navy, and the DHA Director require that their Hub Directors review the insider threat incidents that we determined should have been reported to DITMAC and report those incidents as required (Recommendations 1, 2, and 6). To facilitate those reviews, we provided Hub officials with a list of the incidents reviewed from each of their respective Hubs.

## **(U) USD(I&S) Did Not Provide Oversight of the DoD Insider Threat Program**

(U) The USD(I&S) did not provide oversight of the DoD Insider Threat Program as required by DoD Directive 5205.16. As the DoD senior official with primary oversight responsibilities for the DoD's Insider Threat Program, the USD(I&S) should establish a system of controls to ensure that the DoD Components are reporting insider threat incidents that involve a covered person and meet one or more of the DITMAC Reporting Thresholds.

*(U) The USD(I&S) should establish a system of controls to ensure that the DoD Components are reporting insider threat incidents that involve a covered person and meet one or more of the DITMAC Reporting Thresholds.*

(U) In March 2017, the USD(I&S) issued a memorandum directing the DCSA Director to establish an Insider Threat Enterprise Program Management Office within

DITMAC to assist with the management of the DoD Insider Threat Program.<sup>16</sup>

The memorandum states that the Enterprise Program Management Office is responsible for, among other responsibilities, assessing DoD Component compliance with national and DoD policies and requirements, and recommending improvements. That responsibility, if properly implemented, could provide oversight of the DoD Insider Threat Program and improve Hub compliance with the incident reporting requirements, but as of February 2022, the Enterprise Program Management Office had not initiated an assessment process. Therefore, we recommend that the USD(I&S), in coordination with the DCSA Director and DITMAC Director, ensure

<sup>16</sup> (U) OUSD(I&S) Memorandum for Director, Defense Security Service (now the Defense Counterintelligence and Security Agency [DCSA]), "Establishment of an Insider Threat Enterprise Program Management Office," March 9, 2017.



(U) that the Enterprise Program Management Office establishes and implements a process for assessing DoD Component compliance with the insider threat reporting requirements (Recommendation 3.a.).

### (U) USD(I&S) Did Not Establish Timelines for Reporting Insider Threat Incidents to DITMAC

(U) The USD(I&S) did not establish timelines in DoD Instruction 5205.83 for reporting insider threat incidents to DITMAC. Of the 115 insider threat incidents that the Army, Navy, Marine Corps, DLA, and DHA reported to DITMAC, the time it took the Hubs to report the incidents ranged from 1 day to over 2 years. The insider threat incidents that were reported to DITMAC included incidents involving sexual assault, sexual harassment, aggravated assault, domestic violence, workplace violence, and misuse of technology. Timely reporting is imperative to ensure that the incident receives DoD-wide awareness to assist with the deterrence and prevention of insider threat incidents. Therefore, to ensure that DoD Components are reporting all insider threat incidents that merit DoD-wide awareness to DITMAC in a timely manner, we recommend that the USD(I&S), in coordination with the DCSA Director and DITMAC Director, establish a policy with timelines for DoD Components to report insider threats to DITMAC (Recommendation 3.b.).

*(U) The USD(I&S) did not establish timelines in DoD Instruction 5205.83 for reporting insider threat incidents to DITMAC.*

**(CUI)** [Redacted]

**(CUI)** [Redacted]

*(CUI)* [Redacted]

17 [Redacted]

(CUI)

Therefore, we recommend that the USCYBERCOM Commander require that his Hub Director review the insider threat incidents received since the establishment of their Hubs and report incidents that involve a covered person and meet one or more of the reporting thresholds to DITMAC (Recommendations 4). We also recommend that the NRO and NSA Directors require that their Hub Directors review the insider threat incidents received since the 2016 DoD Component reporting requirement was initiated and report incidents that involve a covered person and meet one or more of the reporting thresholds to DITMAC (Recommendations 5, and 7).

## (U) The DoD Is at Risk of Not Identifying or Mitigating Critical Insider Threats

(U) Insider threat incidents have resulted in harm to the United States and the DoD through espionage, terrorism, unauthorized disclosure of national security information, and the loss or degradation of DoD resources and capabilities. DITMAC was established to provide an enterprise-level capability for managing and analyzing DoD-wide insider threat information. According to the Center for Development of Security Excellence's annual DoD Insider Threat training, research has consistently shown that malicious acts by insiders are seldom impulsive, but instead evolve over time, transforming a trusted insider into a malicious one. Unless the DoD Component Hubs consistently report insider threat incidents to DITMAC as required, DITMAC cannot fully accomplish its mission to provide the DoD with a centralized capability to identify, mitigate, and counter insider threats and reduce the harm to the United States and the DoD by malicious insiders.

*(U) Unless the DoD Component Hubs consistently report insider threat incidents to DITMAC as required, DITMAC cannot fully accomplish its mission to provide the DoD with a centralized capability to identify, mitigate, and counter insider threats and reduce the harm to the United States and the DoD by malicious insiders.*

### (U) Other Matters of Interest

(U) During the audit, we identified that the USD(I&S) has not submitted DoD Insider Threat Program reports to the Secretary of Defense as required by DoD Directive 5205.16. Specifically, the Directive requires the USD(I&S) to monitor, and report to the Secretary of Defense, the progress in implementing the DoD Insider Threat Program in accordance with the National Insider Threat Task Force (NITTF) minimum standards. The NITTF minimum standards state that the report should include details on the insider threat program accomplishments, resources allocation, risks to the agency, recommendations and goals for improvement, and major impediments or challenges. The NITTF minimum standards require that the first annual report be provided to the head of the agency 1 year after the agency has an approved insider threat implementation plan and annually thereafter.

*(U) During the audit, we identified that the USD(I&S) has not submitted DoD Insider Threat Program reports to the Secretary of Defense as required by DoD Directive 5205.16. Specifically, the Directive requires the USD(I&S) to monitor and report to the Secretary of Defense, the progress in implementing the DoD Insider Threat Program in accordance with the National Insider Threat Task Force (NITTF) minimum standards.*

(U) The DoD insider threat implementation plan was approved in July 2019; therefore, the USD(I&S) should have submitted a report to the Secretary of Defense for FYs 2020 and 2021. When we inquired about the status of the reports, OUSD(I&S) officials stated that the FY 2020 report was canceled due to processing delays and they were currently drafting the FY 2021 report. Therefore, we recommend that the USD(I&S), in coordination with the DCSA Director and DITMAC Director, submit the FY 2021 annual report on the DoD Insider Threat Program to the Secretary of Defense and establish a process for ensuring that subsequent reports are submitted in accordance with NITTF minimal standards and DoD Directive 5205.16 (Recommendation 3.c.).

## **(U) Recommendations, Management Comments, and Our Response**

### **(U) Revised Recommendations**

~~(CUI)~~ As a result of management comments, we revised Recommendations 5 and 7 to require the NRO and NSA Hub Directors to review the insider threat incidents received since the 2016 DoD Component reporting requirement was initiated instead of the Hubs' establishment [REDACTED].

### **(U) Recommendation 1**

**(U) We recommend that the Secretary of the Army require that the Army Insider Threat Hub Director review the insider threat incidents that we determined should have been reported to the DoD Insider Threat Management and Analysis Center and report those incidents as required.**

### **(U) Department of the Army Comments**

(U) The Under Secretary of the Army, responding for the Secretary of the Army, agreed, stating that the Army completed all recommended actions. The Under Secretary stated that the Army Insider Threat Hub Director completed a review of the unreported insider threat incidents identified in this report and submitted all nine incidents to DITMAC in July 2022. The Under Secretary also stated that the Army remains ready to work with the USD(I&S) as it establishes specific timelines for the DoD Components to submit insider threat incidents to DITMAC.

### **(U) Our Response**

(U) Comments from the Under Secretary addressed the specifics of the recommendation. We verified that the Army Insider Threat Hub submitted all unreported incidents identified in our report to DITMAC, as required. Therefore, the recommendation is closed, and no further comments are required.

### **(U) Recommendation 2**

**(U) We recommend that the Secretary of the Navy require that the Navy Insider Threat Hub Director, in coordination with the Navy and Marine Corps Insider Threat Hubs, review the insider threat incidents that we determined should have been reported to the DoD Insider Threat Management and Analysis Center and report those incidents as required.**

### ***(U) Department of the Navy Comments***

(U) The Deputy Under Secretary of the Navy for Intelligence and Security, responding for the Secretary of the Navy, agreed, stating that the Navy and Marine Corps Hubs reviewed their respective unreported insider threat incidents identified in our report and submitted all incidents to DITMAC in June 2022 and July 2022, respectively.

(U) The Deputy Under Secretary added that although the Navy and Marine Corps were operating as one Insider Threat Hub during the audit, the Deputy Under Secretary of the Navy decided to separate the Navy and Marine Corps Hubs in July 2022. The Deputy Under Secretary explained that Navy and Marine Corps Hubs have begun the process to update their respective service instructions and standard operating procedures to reflect this change, which the Navy believes will ensure that future insider threat incidents are reported to DITMAC, as required.

### ***(U) Our Response***

(U) Comments from the Deputy Under Secretary addressed the specifics of the recommendation. We verified that the Navy and Marine Corps Insider Threat Hubs submitted all unreported insider threat incidents identified in our report to DITMAC, as required. Therefore, the recommendation is closed, and no further comments are required.

### ***(U) Recommendation 3***

**(U) We recommend that the Under Secretary of Defense for Intelligence and Security, in coordination with the Defense Counterintelligence and Security Agency Director and the DoD Insider Threat Management and Analysis Center Director,**

- a. **(U) Ensure that the Enterprise Program Management Office establishes and implements a process for assessing DoD Component compliance with insider threat reporting requirements.**
- b. **(U) Establish a policy with timelines for DoD Components to report insider threats to the DoD Insider Threat Management and Analysis Center.**
- c. **(U) Submit the FY 2021 annual report on the DoD Insider Threat Program to the Secretary of Defense and establish a process for ensuring that subsequent reports are submitted in accordance with the National Insider Threat Task Force Minimum Standards for Insider Threat Programs and DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, (Incorporating Change 2, August 28, 2017).**

### ***(U) Under Secretary of Defense for Intelligence and Security Comments***

(U) The DoD Counter-Insider Threat Deputy Director, responding for the OSD(I&S), agreed with Recommendations 3.a. and 3.b., stating that the OSD(I&S) and DITMAC will incorporate the necessary changes in the current draft of DoD Directive 5205.16 and the associated DoD Manual. The Deputy Director added that the planned release for the updated Directive and Manual would be in the third quarter of FY 2023. The Deputy Director partially agreed with Recommendation 3.c. stating that the FY 2021 annual DoD Insider Threat Program report is still in draft. Therefore, the OSD(I&S) and DITMAC will not submit the FY 2021 report but instead, incorporate its content in the FY 2022 report. The Deputy Director added that the OSD(I&S) plans to staff the FY 2022 annual report by the end of the second quarter of FY 2023. The Deputy Director explained that future annual reports would be staffed by the second quarter of the following FY covered by the report.

### ***(U) DoD Insider Threat Management and Analysis Center Comments***

(U) Although not required to comment, the DITMAC Deputy Chief agreed, stating that DITMAC is currently developing an Insider Threat Assessment Program through its Enterprise Program Management Office. The Deputy Chief explained that the Enterprise Program Management Office personnel would evaluate all DoD Insider Threat Programs based on risk-management criteria to be included in the revised DoD Directive 5205.16. The Deputy Chief added that DITMAC plans to start the evaluations in the first quarter of FY 2023.

### ***(U) Our Response***

(U) Comments from the Deputy Director addressed the specifics of Recommendations 3.a. and 3.b.; therefore, the recommendations are resolved but remain open. We will close the recommendations once OSD(I&S) officials provide us with documentation verifying that they updated DoD Directive 5205.16 and the associated DoD Manual, including updates to the DoD Component review process, incident reporting timeframes, and the annual reporting process. We also request that OSD(I&S) officials provide us with documentation verifying that DITMAC initiated the DoD Component Insider Threat Assessment Program.

(U) Although the Deputy Director partially agreed with Recommendation 3.c., the comments provided addressed the specifics of the recommendation; therefore, the recommendation is resolved but remains open. We agree that the OSD(I&S) should focus on submitting the FY 2022 annual DoD Insider Threat Program report and ensure the timely submission of future annual reports to the Secretary

(U) of Defense. We will close the recommendation once we obtain and review documentation from OUSD(I&S) officials showing that they submitted the FY 2022 annual report to the Secretary of Defense.

**Recommendation 4**

**(U) We recommend that the Commander of the U.S. Cyber Command require that the U.S. Cyber Command Insider Threat Hub Director, in coordination with the National Security Agency Insider Threat Hub Director, review the insider threat incidents received since the establishment of the Hub and report incidents that involve a covered person and meet one or more of the reporting thresholds to the DoD Insider Threat Management and Analysis Center.**

***(U) U.S. Cyber Command Comments***

~~(CUI)~~ The USCYBERCOM Chief of Staff, responding for the USCYBERCOM Commander, agreed, [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

***(U) Our Response***

~~(CUI)~~ Comments from the Chief of Staff addressed the specifics of recommendation; therefore, the recommendation is resolved but remains open. We will close the recommendation once the Chief of Staff provides documentation verifying that [REDACTED]  
[REDACTED]  
[REDACTED]

**(U) Recommendation 5**

**(U) We recommend that the National Reconnaissance Office Director require that the National Reconnaissance Office Insider Threat Hub Director review the insider threat incidents received since the 2016 DoD Component reporting requirement was initiated and report incidents that involve a covered person and meet one or more of the reporting thresholds to the DoD Insider Threat Management and Analysis Center.**

### *(U) National Reconnaissance Office Comments*

~~(U)~~ The NRO Director disagreed [REDACTED]

~~(U)~~ [REDACTED]

### *(U) Our Response*

~~(U)~~ Based on management comments, we revised the recommendation to state that the NRO should review and report applicable insider threat incidents to DITMAC since the USD(I&S) established the DoD Component reporting requirement in December 2016 instead of the NRO Hub's establishment [REDACTED]. However, that revision does not affect our response to the NRO Director's comments, which is that the NRO Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved.

~~(U)~~ As stated in this report, the USD(I&S) directed all DoD Components to report insider threat incidents involving a covered person that meet one or more of the reporting thresholds to DITMAC in the December 2016 memorandum. The memorandum does not waive that requirement for any DoD Component and does not discuss alternative reporting methods in lieu of reporting incidents to DITMAC. Furthermore, the FY 2017 National Defense Authorization Act revised the definition of a DoD insider to include **any person who has, or once had, authorized access to DoD information, facilities, networks, or other resources** [emphasis added].



~~(U)~~ [Redacted]  
[Redacted]  
[Redacted]

(U) We request that the NRO Director provide comments on the final report, stating the NRO’s plan for reviewing insider threat incidents since the 2016 DoD Component reporting requirement was initiated and to ensure that the Hub reports all future incidents that involve a covered person and meet one or more of the reporting thresholds to DITMAC.

***(U) Recommendation 6***

**(U) We recommend that the Defense Health Agency Director require that the Defense Health Agency Insider Threat Hub Director review the insider threat incidents that we determined should have been reported to the DoD Insider Threat Management and Analysis Center and report those incidents as required.**

***(U) Management Comments Required***

(U) The DHA Director did not respond to the recommendation; therefore, the recommendation is unresolved. We request that the Director provide comments on the final report.

***(U) Recommendation 7***

**(U) We recommend that the National Security Agency/Central Security Service Director require that the National Security Agency Insider Threat Hub Director review the insider threat incidents received since the 2016 DoD Component reporting requirement was initiated and report incidents that involve a covered person and meet one or more of the reporting thresholds to the DoD Insider Threat Management and Analysis Center.**

***(U) National Security Agency Comments***

~~(U)~~ The Chief of Staff for Workforce Support Activities, responding for the NSA/Central Security Service Director, disagreed, [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

(CUI) [REDACTED]

### *(U) Our Response*

(CUI) Based on management comments, we revised the recommendation to state that the NSA should review and report applicable insider threat incidents to DITMAC since the USD(I&S) established the DoD Component reporting requirement in December 2016 instead of the NSA Hub's establishment [REDACTED]. However, that revision does not affect our response to the Chief of Staff's comments in which the Chief of Staff did not address the specifics of the recommendation; therefore, the recommendation is unresolved.

(CUI) As stated in this report, the USD(I&S) directed all DoD Components to report insider threat incidents involving a covered person that meet one or more of the reporting thresholds to DITMAC in the December 2016 memorandum. The memorandum does not waive that requirement for any DoD Component, and does not state that the DoD Components should identify and report only those incidents that they consider the most significant and concerning cases. Furthermore, the FY 2017 National Defense Authorization Act revised the definition of a DoD insider to include **any person who has, or once had, authorized access to DoD information, facilities, networks, or other resources** [emphasis added]. [REDACTED]

(U) We request that the NSA Director provide comments on the final report stating NSA's plan for reviewing insider threat incidents since the 2016 DoD Component reporting requirement was initiated, and to ensure that the Hub reports all future incidents that involve a covered person and meet one or more of the reporting thresholds to DITMAC.

## (U) Appendix A

---

### (U) Scope and Methodology

(U) We conducted this performance audit from January 2020 through June 2022 in accordance with generally accepted government auditing standards.<sup>19</sup> Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our audit objective. We concluded that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

(U) We met with officials from the OUSD(I&S), DITMAC, Defense Intelligence Agency, and NITTF to discuss their roles and responsibilities for the DoD Insider Threat Program. We sent request for information or met with personnel from seven DoD Component Insider Threat Hubs—the Army, Navy, Marine Corps, DLA, DHA, NRO, and USCYBERCOM—to review their insider threat programs and reporting processes. Although the Department of the Navy considers itself as one insider threat hub, we observed the Navy running two separate insider threat Hubs and reporting incidents separately to DITMAC. Therefore, we treated the Navy and the Marine Corps Hubs as separate Hubs.

~~(CUI)~~ We obtained insider threat incident data from five of the DoD Component Insider Threat Hubs (Army, Navy, Marine Corps, DLA, and DHA) to evaluate whether the Hubs reported the insider threat incidents involving a covered person that met the reporting thresholds to DITMAC. [REDACTED]  
[REDACTED]  
[REDACTED]

(U) The universe for our review was the insider threat incidents reported from February 2016 to March 2021 to the five DoD Component Hubs reviewed. We selected two nonstatistical samples of insider threat incidents reported to each of the selected Hubs. We used the first sample of insider threat incidents to verify whether the Hubs reported the incidents to DITMAC as indicated by their internal tracking system or spreadsheets. We used the second sample of potential insider threat incidents reported to Hubs to determine whether any of the incidents that were not reported to DITMAC involved a cover person and met one or more of the DITMAC Reporting Thresholds.

---

<sup>19</sup> (U) We suspended the project from May to August 2020 due to the impact of the coronavirus disease-2019 pandemic.

(U) For the first sample, we reviewed the Hub's internal tracking system or spreadsheets to identify incidents that were reported to DITMAC as indicated by the Hub. We then selected a nonstatistical sample to verify whether the incidents were reported to DITMAC by reviewing DSoS.<sup>20</sup> We also identified the length of time it took for the Hubs to report the incidents to DITMAC by comparing the date the Hub received the incident to when officials reported the incident in DSoS.

(U) For the second sample, we reviewed the Hub's internal tracking system or spreadsheets to identify incidents that were not reported to DITMAC as indicated by the Hub. We filtered the information in the tracking systems or spreadsheets to identify incidents that the Hub indicated as having met one of the reporting thresholds and, if a risk category was assigned, the incidents categorized as high risk. We then selected a nonstatistical sample of incidents and reviewed the associated information or case files to determine how the Hubs reviewed and analyzed the incidents.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any comments submitted by the DoD Components about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

## **(U) Use of Computer-Processed Data**

(U) We obtained a list of insider threat incidents from the five DoD Component Hubs reviewed to determine the universe of incidents. The Hubs provided us with a listing of incidents in Microsoft Excel worksheets. To assess the reliability of the data, we verified whether a nonstatistical sample of incidents that were indicated by the Hubs as being reported to DITMAC by confirming the existence of the incident in DSoS. We also discussed the worksheets with the Hubs to further assess the reliability of the information and verified information contained in the case files for the incidents reviewed. Therefore, we determined that worksheets were sufficiently reliable for the purposes of this audit to determine whether the Hubs reported insider threat incidents involving a covered person that met one or more of the reporting thresholds to DITMAC.

---

<sup>20</sup> (U) DSoS supports DoD Components and is the primary tool for capturing, consolidating, storing, analyzing, and managing insider threat data.

## **(U) Use of Technical Assistance**

(U) We received assistance from the DoD OIG Quantitative Methods Division to develop our nonstatistical samples of insider threat incidents to review.

## **(U) Prior Coverage**

(U) During the last 5 years, the DoD OIG and Naval Audit Service issued two reports discussing the DoD's Insider Threat Program.

### **(U) DoD OIG**

(U) Report No. DODIG-2019-107, "Evaluation of Combatant Commands' Insider Threat Programs," July 30, 2019 (Report is SECRET//NOFORN)

(U) The report is classified.

### **(U) Navy**

(U) Report No. N2019-0002, "Department of the Navy's Insider Threat Program," October 12, 2018 (Report is CUI)

(~~CUI~~) [REDACTED]  
[REDACTED]  
[REDACTED]

## (U) Appendix B

---

### (U) DoD Insider Threat Incidents

(U) Since 2001, DoD insiders have made high-profile disclosures of data critical to national security. The following are examples of DoD insider threat incidents.

- (U) The September 21, 2001 arrest of Ana Montes, a former Defense Intelligence Agency senior analyst, who pleaded guilty to conspiring to commit espionage after providing information to the Cuban Government.
- (U) The June 2013 leak of highly classified NSA documents to the media by ex-CIA employee and NSA contractor Edward Snowden. The documents revealed numerous global surveillance programs run by the NSA.<sup>21</sup>
- (U) The July 2013 court-martial conviction of Chelsea Manning, a former U.S. Army Intelligence Analyst, who violated the Espionage Act and other offenses, after disclosing nearly 700,000 classified and sensitive documents to WikiLeaks.<sup>22</sup>
- (U) The September 2013 Washington Navy Yard Shooting by Aaron Alexis, a Defense contractor and former Navy reservist. The contractor, who had a secret security clearance, killed 12 U.S. Navy civilian and contractor employees and wounded 4 others before being shot and killed by law enforcement officers at the Washington Navy Yard in Washington, D.C.
- (U) The August 2016 arrest of Harold Thomas Martin III, a former contractor for Booz Allen Hamilton working for the NSA, who pleaded guilty for the willful retention of national defense information.
- (U) The December 2019 Pearl Harbor Naval Shipyard shooting of three people by an active duty U.S. Navy sailor, killing two DoD civilians and injure another before killing himself at the Pearl Harbor Naval Shipyard in Pearl Harbor, Hawaii.
- (U) The December 2019 Naval Air Station Pensacola terrorist attack, in which 11 people were shot by a second lieutenant of the Royal Saudi Air Force. The second lieutenant, a foreign military student in aviation training, killed three U.S. Navy Sailors and injured eight others before being killed by Escambia County sheriff deputies at Naval Air Base Pensacola in Pensacola, Florida. On January 13, 2020, the Department of Justice classified the incident as an act of terrorism motivated by “jihadist ideology.” On February 2, 2020, Al-Qaeda in the Arabian Peninsula claimed responsibility for the shooting, stating that it had directed the attack.

---

<sup>21</sup> (U) Edward Snowden, a former NSA contractor, was charged on June 14, 2013, with theft of government property and two counts of violating the Espionage Act after leaking highly classified NSA documents to the media.

<sup>22</sup> (U) In 2014, Bradley Manning legally changed his name to Chelsea Manning, which was reflected in all military and court documents.

- (U) The October 2021 arrest of Jonathan Toebbe, a U.S. Navy nuclear engineer, and his wife for trying to sell restricted data concerning the design of nuclear-powered warships to an individual they believed was a representative of a foreign power, but was instead an undercover Federal Bureau of Investigation agent.

## (U) Appendix C

---

### (U) DITMAC Reporting Thresholds

(U) In December 2016, the USD(I&S) published the list of the 13 DITMAC Reporting Thresholds.<sup>23</sup> The thresholds are a guide for DoD Component Hubs to use when determining whether an incident involved a covered person (DoD insider) and should be reported as an insider threat to DITMAC. See the details for the 13 reporting thresholds below.

**(U) Threshold 1: Serious Threat.** Information pertaining to any serious threat covered persons may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. Serious threats are defined as those that present a reasonable risk to life or limb, or have the potential to degrade or destroy a critical intelligence or operational capability of DoD.

**(U) Threshold 2: Allegiance to the United States.** Information pertaining to any covered person exhibiting questionable allegiance to the United States through words or actions to include involvement in, support of, training to commit, or advocacy of any act of sabotage, treason, or sedition against the United States. An allegiance concern arises when a covered person acts or prepares to act on beliefs in a manner that violates the law. Criticism of the U.S. Government is protected by freedom of speech and the expression of unpopular or anti-government beliefs do not show lack of allegiance. However, covered persons do not have the right to engage in force or violence, either actual or threatened, or violate the law in any other way to further their beliefs.

**(U) Threshold 3: Espionage/Foreign Considerations.** The investigation, arrest, or apprehension by a federal law enforcement agency, Military Department Counterintelligence Organization, and/or DoD Component's Counterintelligence element of any covered person for espionage. Investigations into and/or judicial or administrative actions taken against any covered person regarding reportable Foreign Intelligence Entity contacts, activities, indicators, and behaviors as detailed in DoD Directive 5240.06. Information pertaining to any covered person suspected to have unauthorized contact with an officer or agent of a Foreign Intelligence Entity, or who fails to report or disclose, when required to do so: any previous or ongoing relationship or contact with any person from a foreign country; foreign travel; foreign passport or identity card; foreign citizenship or foreign residency; foreign military service; ownership of foreign property; or, undue influence by a foreign interest (for example, on-going personal or professional foreign contacts; receipt of benefits from a foreign country).

---

<sup>23</sup> (U) USD(I&S) "DITMAC Reporting Thresholds: Desk Reference Guide," issued on December 2016.



**(U) Threshold 4: Personal Conduct.** Information, in regard to a covered person, pertaining to deliberate omission, concealment, or falsification of relevant facts from any personnel security investigations, polygraph examinations (including counterintelligence scope and expanded screening scope polygraphs), or a pattern of behavior (two or more incidents closely related in time) that puts the individual's judgment, trustworthiness, candor, honesty or willingness to comply with applicable laws and regulations into question.

**(U) Threshold 5: Behavioral Considerations.** Information pertaining to a covered person who exhibits behaviors that cast doubts on their judgment, reliability, or trustworthiness. Such behaviors include emotionally unstable, irresponsible, dysfunctional, violent, paranoid, bizarre, anti-social, or aggressive behavior. This also includes information derived from User Activity Monitoring, human resources information, military and civilian performance evaluations, and reports of criminal or family law proceedings that indicate a person cleared by DoD is a threat to him or herself. Seeking mental health counselling is not by itself a reporting threshold.

**(U) Threshold 6: Criminal Conduct.** The investigation, arrest or apprehension by a federal, state, or local, law enforcement agency, or the conviction, indictment, or charging by a federal, state or local jurisdiction of any covered person involving: the loss of life; actual or suspected acts of violence or threats of violence (including sexual assault); the illegal possession or transfer of weapons of mass destruction; and any criminal offenses involving the use of weapons or explosives.

**(U) Threshold 7: Unauthorized Disclosure.** Information that indicates a covered person is knowingly involved in unauthorized disclosure, theft, loss, or compromise of classified or protected information to a foreign power, an agent of foreign power, the media, or any unauthorized recipient. Reportable unauthorized disclosures include unauthorized publication of classified or controlled unclassified information present in books, articles, or other written, online, or broadcast media sources determined to have been written or otherwise provided by current or former cleared DoD-affiliated officials.

**(U) Threshold 8: Unexplained Personnel Disappearance.** The suspicious death or unexplained disappearance of any covered person.

**(U) Threshold 9: Handling Protected Information.** Information pertaining to a covered person deliberately mishandling protected information, or exhibiting a pattern (two or more incidents closely related in time) of negligent noncompliance with rules, procedures, guidelines, or regulations for protecting classified or controlled unclassified information.

**(U) Threshold 10: Misuse of Information Technology.** Information pertaining to a covered person deliberately misusing information technology, or exhibiting a pattern (two or more incidents closely related in time) of negligent noncompliance with rules, procedures, guidelines or regulations pertaining to information technology.

**(U) Threshold 11: Terrorism.** Information pertaining to a covered person providing support to, or who is in contact (through on-line, e-mail, or social net-working) with known or suspected domestic or international terrorist or extremist individuals, organizations, or groups. Any attempt or conspiracy to commit the above shall also be reported.

**(U) Threshold 12: Criminal Affiliations.** Information pertaining to a covered person providing support to, or who are in contact (to include on-line, e-mail, and social net-working) with known or suspected domestic or international criminal organizations, criminal street gangs, or groups engaged in racketeering activities. Any attempt or conspiracy to conduct the above shall also be reported. Affiliation by covered persons with eco-terrorist organizations, animal rights extremist organizations and sovereign citizen extremist groups are best captured under the terrorism threshold.

**(U) Threshold 13: Adverse Clearance Actions.** The suspension, revocation, or denial of a security clearance for reasons identified in thresholds 1-12. Incidents that meet this threshold must meet another DITMAC threshold.

## (U) Management Comments

### (U) Department of the Army



UNDER SECRETARY OF THE ARMY  
WASHINGTON

AUG 16 2022

MEMORANDUM FOR Department of Defense Office of Inspector General, 4800 Mark Center Drive, Alexandria, VA 22350-1500

Subject: DOD Inspector General Audit of the Department of Defense Component Insider Threat Reporting to the Department of Defense Insider Threat Management and Analysis Center, (Project D2020-D000CP-0074)

1. I have reviewed the Department of Defense (DoD) Inspector General report. The Army concurs with the auditor's recommendation and has completed the actions necessary to it.
2. You recommended that the Secretary of the Army require that the Army Insider Threat Hub Director review the insider threat incidents that you determined should have been reported to the DoD Insider Threat Management and Analysis Center, and report those incidents as required.
3. As of 29 July 2022, the Army Hub Director, Headquarters, Department of the Army G-3/5/7, completed its review of the incidents and reported the nine flagged in the report to the DoD Insider Threat Management and Analysis Center (DITMAC). The Army remains ready to work with Under Secretary of Defense for Intelligence and Security as it establishes specific timelines for the DoD Components to submit reports of insider threat incidents.
4. The point of contact for this action is [REDACTED]

  
Gabe Camarillo

## (U) Department of the Navy



DEPUTY UNDER SECRETARY OF THE NAVY  
INTELLIGENCE AND SECURITY  
WASHINGTON DC 20350-1000

5041  
Ser 019  
2 Aug 22

From: Deputy Under Secretary of the Navy for Intelligence and Security  
To: Department of Defense Office of Inspector General

Subj: DEPARTMENT OF THE NAVY RESPONSE TO RECOMMENDATION 2 OF AUDIT  
OF THE DOD COMPONENT INSIDER THREAT REPORTING TO THE DOD  
INSIDER THREAT MANAGEMENT AND ANALYSIS CENTER (PROJECT NO.  
D2020-D000CP-0074.000)

Ref: (a) SECNAVINST 5510.37A  
(b) USD(I) Memorandum, "Reporting Information to the Department of Defense Insider  
Threat Management and Analysis Center," December 29, 2016  
(c) OPNAVINST 5510.165B  
(d) MCO 5510.21

1. This letter provides the response on behalf of the Department of the Navy (DON) to Recommendation 2 of the Audit of the DoD Component Insider Threat Reporting to the DoD Insider Threat Management and Analysis Center (Project No. D2020-D000CP-007444.000) Report and input on the appropriate classification/marketing of the report. Recommendation 2 states: "[w]e recommend that the Secretary of the Navy require that the Navy Insider Threat Hub Director, in coordination with the Navy and Marine Corps Insider Threat Hubs, review the insider threat incidents that we determined should have been reported to the DoD Insider Threat Management and Analysis Center and report those incidents as required."

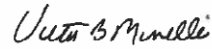
2. DON Response: Concur with Recommendation 2 and no additional changes to existing security markings on the report beyond those already present are recommended. The Navy Insider Threat Program (Navy InTP) and Marine Corps Counter Insider Threat Program (MCCInTP) conducted internal reviews of their respective 26 and 30 insider threat incidents identified in the subject audit. Consistent with internal procedures Navy InTP and MCCInTP reported these incidents between April 2021 and the conclusion of the audit as the reporting requirement for each incident was identified. The Navy InTP reported completion as of 7 June 2022 and the MCCInTP reported completion as of 15 July 2022.

3. During the period of the audit, DON insider threat analysis and response capabilities were consolidated within a single analytic hub pursuant to reference (a), which directed compliance with the DITMAC reporting thresholds listed in reference (b). Effective 5 July 2022, the Deputy Under Secretary of the Navy for Intelligence and Security (DUSN (I&S)) divested the analysis and response capabilities of the DON Insider Threat Analytic Hub back to the Navy InTP and MCCInTP. Consequently, the Navy InTP and MCCInTP have initiated the staffing process to change their respective service instructions, references (c) and (d), and standard operating procedures to reflect their assumption of insider threat analysis and response capabilities. Changes will ensure insider threat incidents involving covered personnel that meet one or more reporting thresholds are reported to the DITMAC in the future.

## (U) Department of the Navy (cont'd)

Subj: DEPARTMENT OF THE NAVY RESPONSE TO RECOMMENDATION 2 OF AUDIT OF THE DOD COMPONENT INSIDER THREAT REPORTING TO THE DOD INSIDER THREAT MANAGEMENT AND ANALYSIS CENTER (PROJECT NO. D2020-D000CP-0074.000)

4. The point of contact for this matter is [REDACTED]



V. B. MINELLA

## (U) Under Secretary of Defense for Intelligence and Security



INTELLIGENCE  
AND SECURITY

OFFICE OF THE UNDER SECRETARY OF DEFENSE  
5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
(ATTN: PROGRAM DIRECTOR FOR AUDIT, CYBERSPACE  
OPERATIONS)

SUBJECT: Audit of the DoD Component Insider Threat Reporting to the DoD Insider Threat  
Management and Analysis Center (Project No. D2020-D000CP-0074.000)

Thank you for the opportunity to respond to the Inspector General's draft report and discuss the Department of Defense (DoD) Component Insider Threat Reporting to the DoD Insider Threat Management and Analysis Center (DITMAC). We agree with recommendations 3a.-3c. Please see our comments in the attached.

Our office is working with the DITMAC to address recommendations 3a.-3c. in our current draft of DODI 5205.16, COUNTERING THE INSIDER THREAT IN THE DEPARTMENT OF DEFENSE and associated DoD Manual.

Thanks again for working with us and the Enterprise on these important issues. My primary point of contact is [REDACTED]

A handwritten signature in blue ink, appearing to read "L. Call".

Lewis R. Call  
Deputy Director  
DoD Counter-Insider Threat

Attachment:  
As stated

## (U) Under Secretary of Defense for Intelligence and Security (cont'd)

DoD IG Draft Report Dated July 6, 2022  
Project No. D2020-D000CP-0074.000

Audit of the DoD Component Insider Threat Reporting  
to the DoD Insider Threat Management and Analysis Center

**RECOMMENDATION 3:** That the Under Secretary of Defense for Intelligence and Security, in coordination with the Defense Counterintelligence and Security Agency Director and the DoD Insider Threat Management and Analysis Center Director,

- a. Ensure that the Enterprise Program Management Office establishes and implements a process for assessing DoD Component compliance with insider threat reporting requirements.
- b. Establish a policy with timelines for DoD Components to report insider threats to the DoD Insider Threat Management and Analysis Center.
- c. Submit the FY 2021 annual report on the DoD Insider Threat Program to the Secretary of Defense and establish a process for ensuring that subsequent reports are submitted in accordance with the National Insider Threat Task Force Minimum Standards for Insider Threat Programs and DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, (Incorporating Change 2, August 28, 2017).

**DoD RESPONSE:** Agree. The OUSD(I&S) and DITMAC will incorporate Recommendation 3 requirements and processes in the current draft of DODI 5205.16, COUNTERING THE INSIDER THREAT IN THE DEPARTMENT OF DEFENSE and associated DoD Manual. OUSD(I&S) planned release of the DODI and DODM is Q3, 2023, subject to the DoD staffing process.

## (U) DoD Insider Threat Management and Analysis Center



**DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY  
DEFENSE INSIDER THREAT MANAGEMENT AND ANALYSIS CENTER  
1550 CRYSTAL DRIVE  
ARLINGTON VA 22202**

August 5, 2022

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

**SUBJECT:** Response to Draft Report of the Audit of the DoD Component Insider Threat Reporting to the DoD Insider Threat Management and Analysis Center (Project No. D2020-D000CP-0074.000)

The DITMAC has no issues, edits or comments on the subject draft report. Additionally we concur with all of the recommendations and specifically that the DITMAC's Enterprise Program Management Office (EPMO) establishes and implements a process for assessing DoD Component compliance with insider threat reporting requirements. The markings and portion-markings are accurate and reflect the status of CUI related to the DITMAC.

Reference the reports recommendation 3A, the DITMAC is currently developing an Insider Threat Assessment Program through the DITMAC's Enterprise Program Management Office. EPMO personnel will evaluate all DoD Insider Threat programs based on appropriate risk-management criteria outlined in the enhanced Full Operating Capabilities to be codified in the revised DOD Directive 5205.16. The initial assessment is currently being coordinated and will occur in the 1<sup>st</sup> QTR FY23

*Mark Burns* BURNS.MARK.AL Digitally signed by  
Mark Burns LEN. [REDACTED]  
Deputy Chief, Enterprise Program Management Office  
Defense Insider Threat Management and Analysis Center



# (U) U.S. Cyber Command



~~CUI~~  
DEPARTMENT OF DEFENSE  
UNITED STATES CYBER COMMAND  
9800 SAVAGE ROAD, SUITE 6171  
FORT GEORGE G. MEADE, MARYLAND 20755

JUL 22 2022

Reply to:  
Chief of Staff

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

Subject: ~~(CUI)~~ [REDACTED]

Reference: (U) DoDI 5205.83, DoD Insider Threat Management and Analysis Center, 30 March 2017

1. (U) DOD Inspector General (DODIG) requests formal comments from USCYBERCOM authorizing an official response regarding Recommendation 4 from the Audit of the DOD Component Insider Threat Reporting to the DOD Insider Threat Management and Analysis Center Report.
2. (U) DODIG Recommendation 4: We recommend that the Commander of United States Cyber Command require that the USCYBERCOM Insider Threat Hub Director, in coordination with the National Security Agency Insider Threat Hub Director, review the insider threat incidents received since the establishment of the Hub and report incidents that involve a covered person and meet one or more of the reporting thresholds to the DoD Insider Threat Management and Analysis Center.

3. ~~(CUI)~~ [REDACTED]

4. (U) The point of contact for this response is [REDACTED]

BRADLEY L. PYBURN  
Major General, U.S. Air Force  
Chief of Staff

Controlled by: USCYBERCOM  
Controlled by: IAS  
Categories: APSEP  
USCYBERCOM  
FOUO [REDACTED]

~~CUI~~

# (U) National Reconnaissance Office



Office of the Director

~~UNCLASSIFIED//FOUO~~

## NATIONAL RECONNAISSANCE OFFICE

14675 Lee Road  
Chantilly, VA 20151-1715

7 September 2022

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: (U) National Reconnaissance Office Formal Response to Department of Defense Inspector General Audit of the Department of Defense Component Insider Threat Reporting to the Department of Defense Insider Threat Management and Analysis Center, Recommendation 5

REFERENCE: (U) Audit of the DoD Component Insider Threat Reporting to the DoD Insider Threat Management and Analysis Center (DoD IG Project No. D2020-D000CP-0074.000) (U//FOUO)

(U//FOUO)

[Redacted]

(U//FOUO)

[Redacted]

(U//FOUO)

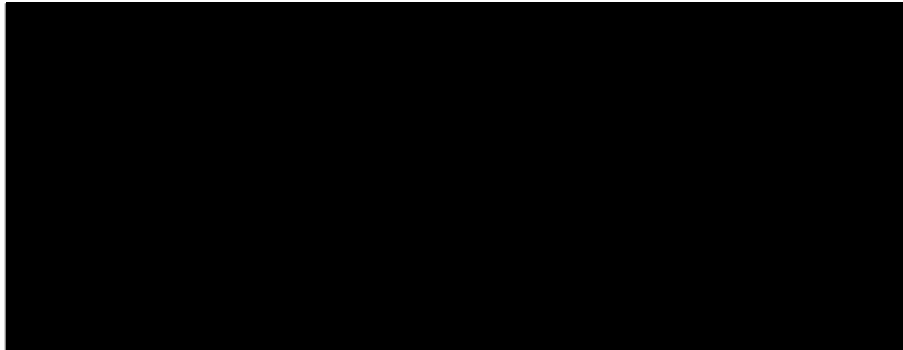
[Redacted]

~~UNCLASSIFIED//FOUO~~

## (U) National Reconnaissance Office (cont'd)

~~UNCLASSIFIED//FOUO~~


SUBJECT: (U) (U) National Reconnaissance Office Formal Response to Department of Defense Inspector General Audit of the Department of Defense Component Insider Threat Reporting to the Department of Defense Insider Threat Management and Analysis Center, Recommendation 5



(U) Please feel free to reach out to my point of contact,



should you have any questions.

  
C.J. Scolese

~~UNCLASSIFIED//FOUO~~

# (U) National Security Agency



NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
FORT GEORGE G. MEADE, MARYLAND 20755

11 August 2022

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

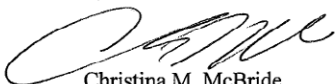
Subject: (U) National Security Agency/Central Security Service's Response to the Department of Defense Inspector General Audit of the Department of Defense Component Insider Threat Reporting to the Department of Defense Insider Threat Management and Analysis Center.

- 1. (U) The Department of Defense Inspector General (DoD OIG) requests formal comments from the National Security Agency/Central Security Service (NSA) authorizing an official response regarding Recommendation 7 from the Audit of the DoD Component Insider Threat Reporting to the DoD Insider Threat Management and Analysis Center (DITMAC).
- 2. (U) The DoD OIG Recommendation 7 provides: We recommend that the National Security Agency/Central Security Service Director require that the National Security Agency Insider Threat Hub Director review the insider threat incidents received since the establishment of the Hub and report incidents that involve a covered person and meet one or more of the reporting thresholds to the DoD Insider Threat Management and Analysis Center.

3. (U//FOUO) [Redacted]

(U//FOUO) [Redacted]

4. (U) The point of contact for this response is [Redacted]

  
Christina M. McBride  
WSA, Chief of Staff

## (U) Acronyms and Abbreviations

---

<b>DCSA</b>	Defense Counterintelligence and Security Agency
<b>DHA</b>	Defense Health Agency
<b>DITMAC</b>	Defense Insider Threat Management and Analysis Center
<b>DLA</b>	Defense Logistics Agency
<b>DSoS</b>	DITMAC System of Systems
<b>JWICS</b>	Joint Worldwide Intelligence Communications System
<b>NITTF</b>	National Insider Threat Task Force
<b>NRO</b>	National Reconnaissance Office
<b>NSA</b>	National Security Agency
<b>OUSD(I&amp;S)</b>	Office of the Under Secretary of Defense for Intelligence and Security
<b>USCYBERCOM</b>	U.S. Cyber Command
<b>USD(I&amp;S)</b>	Under Secretary of Defense for Intelligence and Security



## **Whistleblower Protection**

### **U.S. DEPARTMENT OF DEFENSE**

*Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at [Whistleblowerprotectioncoordinator@dodig.mil](mailto:Whistleblowerprotectioncoordinator@dodig.mil)*

## **For more information about DoD OIG reports or activities, please contact us:**

### **Congressional Liaison**

703.604.8324

### **Media Contact**

[public.affairs@dodig.mil](mailto:public.affairs@dodig.mil); 703.604.8324

### **DoD OIG Mailing Lists**

[www.dodig.mil/Mailing-Lists/](http://www.dodig.mil/Mailing-Lists/)

### **Twitter**

[www.twitter.com/DoD\\_IG](http://www.twitter.com/DoD_IG)

### **DoD Hotline**

[www.dodig.mil/hotline](http://www.dodig.mil/hotline)

**CUI**



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, Virginia 22350-1500  
[www.dodig.mil](http://www.dodig.mil)  
DoD Hotline 1.800.424.9098

**CUI**