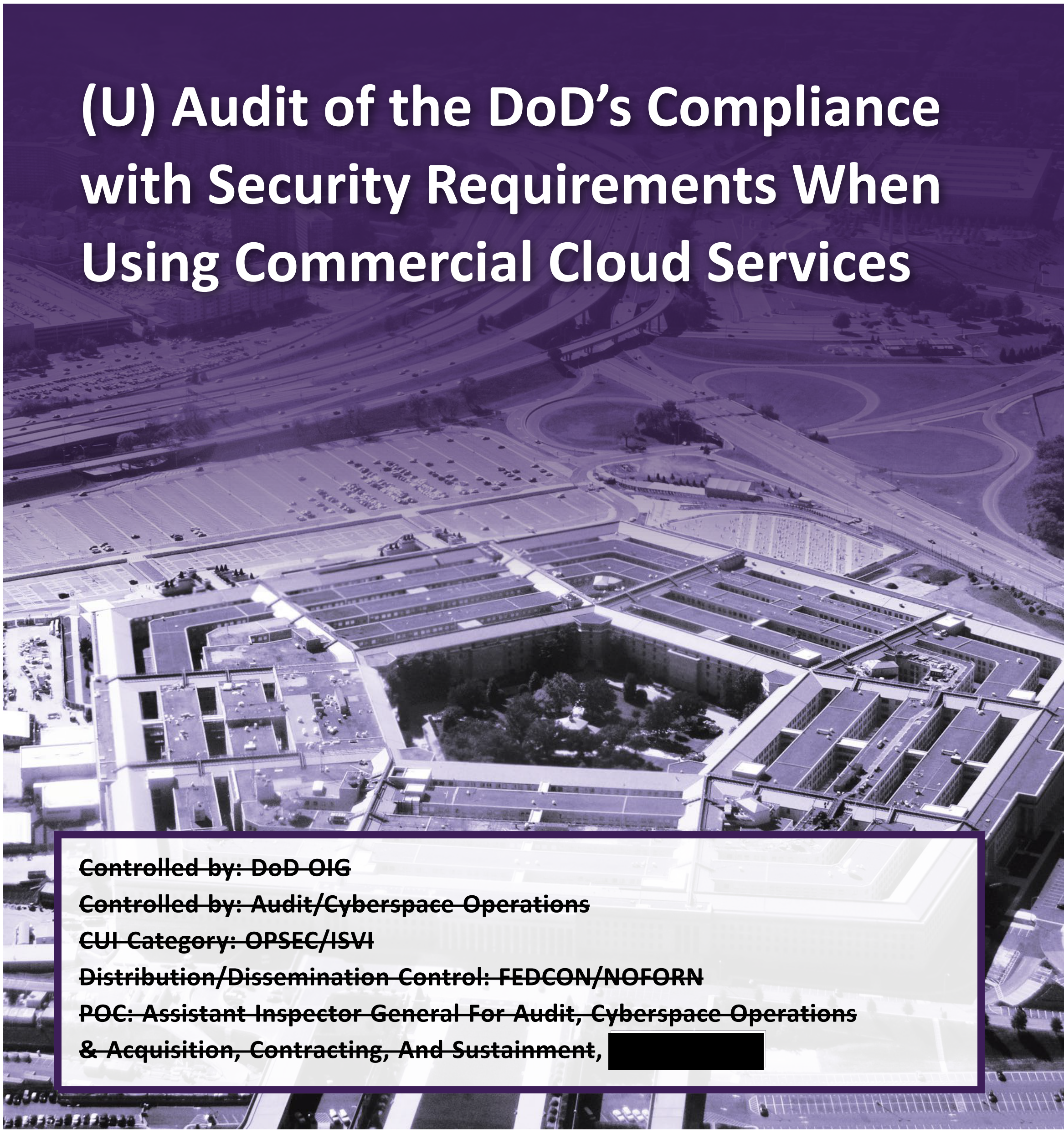
Report No. DODIG-2023-052

~~CUI~~

INSPECTOR GENERAL

*U.S. Department of Defense*

FEBRUARY 15, 2023



# (U) Audit of the DoD's Compliance with Security Requirements When Using Commercial Cloud Services

~~Controlled by: DoD OIG~~

~~Controlled by: Audit/Cyberspace Operations~~

~~CUI Category: OPSEC/ISVI~~

~~Distribution/Dissemination Control: FEDCON/NOFORN~~

~~POC: Assistant Inspector General For Audit, Cyberspace Operations & Acquisition, Contracting, And Sustainment,~~ [redacted]

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

~~CUI~~

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

# (U) Results in Brief

*(U) Audit of the DoD's Compliance with Security Requirements When Using Commercial Cloud Services*

### (U) February 15, 2023

## (U) Objective

(U) The objective of this audit was to determine whether DoD Components complied with Federal and DoD security requirements when using commercial cloud services.

## (U) Background

(U) Since 2011, the DoD has acquired commercial cloud services to meet mission needs. Commercial cloud services allow users to store, access, and share data and software using the Internet rather than locally storing information on servers or computer hard drives. DoD Component authorizing officials (AOs) are responsible for granting the system-level authorization to operate (ATO) when using authorized commercial cloud service offerings (CSOs).

## (U) Findings

(U) The Army, Navy, Air Force, and Marine Corps used three commercial CSOs that were Federal Risk and Authorization Management Program (FedRAMP) and DoD authorized and at the appropriate DoD impact level for the five systems reviewed. However, the AOs did not review all required documentation to consider the commercial CSOs' risks to their systems when granting and reassessing ATOs on a periodic basis thereafter. Specifically, the AOs did not consider system risks that were identified in the supporting documentation of the authorized commercial CSOs' FedRAMP and DoD authorization processes and continuous monitoring activities.

*(U) Findings (cont'd)*

(U) This occurred because all five AOs believed that the FedRAMP and DoD authorization processes were sufficient to mitigate risk to their respective systems. Unless AOs review all required documentation to consider the risks to their respective systems, DoD Components may be unaware of vulnerabilities and cybersecurity risks associated with operating their systems or storing their data in the authorized commercial CSOs.

## (U) Recommendations

(U) We recommend that the Chief Information Officers (CIO) for the Army, Air Force, and Department of the Navy require the AOs to reevaluate the ATOs for the five cloud systems we reviewed. We also recommend that the DoD CIO emphasize the importance of following the DoD Cloud Computing Security Requirements Guide (SRG) when using commercial CSOs. In addition, we recommend that the Defense Information Systems Agency (DISA) Director coordinate with the Joint Authorization Board for FedRAMP to require that commercial cloud service providers remediate all vulnerabilities or provide documentation that describes why the risk to mission impact is low. See the Recommendation section in the body of the report for the full text of all recommendations.

## (U) Management Comments and Our Response

(U) The Army and Department of the Navy CIOs agreed to reevaluate the ATOs for the systems reviewed to ensure compliance with the DoD Cloud Computing SRG. The Air Force Deputy CIO agreed that the Air Force would review and update guidance but did not address whether the AOs would reevaluate the ATOs. Therefore, we request that the Air Force CIO provide comments within 30 days in response to the final report to address reevaluating the ATOs.

(U) The DoD CIO agreed to emphasize the importance of complying with the DoD Cloud Computing SRG and the DISA CIO agreed to continued collaboration with the FedRAMP Joint Authorization Board to ensure cloud service providers remediate vulnerabilities or document risk acceptance.

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

## *(U) Recommendations Table*

| (U)<br>Management | Recommendations Unresolved | Recommendations Resolved | Recommendations Closed |
|---|---|---|---|
| DoD Chief Information Officer | None | 4 | None |
| Director, Defense Information Systems Agency | None | 5 | None |
| Chief Information Officer for the Army | None | 1 | None |
| Department of the Navy Chief Information Officer | None | 2.a and 2.b | None |
| Chief Information Officer for the Air Force | 3 | None | None<br>**(U)** |

(U) Please provide Management Comments by March 17, 2023.

**(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.

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

February 15, 2023

MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT
OF DEFENSE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: (U) Audit of the DoD's Compliance with Security Requirements When Using Commercial Cloud Services (Report No. DODIG-2023-052)

(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 one recommendation that is considered unresolved because management officials did not fully address the recommendation. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendation will remain unresolved until an agreement is reached on the actions to be taken to address the recommendation. Once an agreement is reached, the recommendation 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 recommendation will be closed.

(U) This report contains five 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) 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 to audcso@dodig.mil if unclassified or 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

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations & Acquisition,
Contracting, and Sustainment

# (U) Contents

## (U) Introduction

## (U) Appendixes

## (U) Management Comments

# (U) Introduction

## (U) Objective

(U) The objective of this audit was to determine whether DoD Components complied with Federal and DoD security requirements when using commercial cloud services. See the Appendix for discussion of our scope and methodology, and prior coverage related to the objective.

## (U) Background

(U) Since 2011, the DoD has acquired commercial cloud services to meet mission needs. Commercial cloud services allow users to store, access, and share data and software using the Internet rather than locally storing information on servers or computer hard drives. For example, the DoD uses commercial cloud services to support its missions and other services such as training, munitions inventory, asset and program management, and e-mail. In 2022, the DoD released its Software Modernization Strategy.[1] One of the goals of the strategy is to accelerate the implementation of the DoD enterprise cloud environment by using a multi-cloud, multi-vendor approach to deploy cloud services and ensure that cybersecurity controls and processes are in place to protect DoD data. According to the 2022 DoD Budget Request, the DoD spent approximately $893 million on commercial cloud services in FY 2020, $940 million in FY 2021, and requested over $1.12 billion for FY 2022.[2]

*(U) DoD uses commercial cloud services to support its missions and other services such as training, munitions inventory, asset and program management, and e-mail.*

(U) The National Institute of Standards and Technology (NIST) identifies three types of commercial cloud service offerings (CSOs): Software as a Service, Platform as a Service, and Infrastructure as a Service, each of which provides different services and capabilities.[3]

> **(U) Software as a Service**: Provides a virtual space for users to access software and applications such as Microsoft Office 365 and enterprise e-mail over the Internet, avoiding the need to create, install, and run specific software and applications on the user's computer.

[1] (U) DoD Software Modernization Strategy, February 2, 2022.

[2] (U) "Department of Defense Information Technology and Cyberspace Activities Budget Overview – Fiscal Year 2022 Budget Request," June 2021.

[3] (U) NIST Special Publication 800-145, "The NIST Definition of Cloud Computing," September 2011.

**(U) Platform as a Service**: Provides a virtual space for users to create and control independent applications and data, but the cloud service provider (CSP) delivers and manages the servers, storage, networking, development tools, data analytics, and database management systems.

**(U) Infrastructure as a Service**: Provides a virtual space for users to create and control applications, data, runtime, software, and operating systems, but the CSP provides and manages the physical servers, storage, networking, and visualization of the cloud environment.

## *(U) Federal Requirements for Cloud Security*

(U) In a December 2011 memorandum to all Federal Chief Information Officers, the Office of Management and Budget (OMB) established the Federal Risk and Authorization Management Program (FedRAMP).[4] FedRAMP is a government-wide program that standardizes the security assessment, authorization, and continuous monitoring process for cloud products and services.[5] The Joint Authorization Board (JAB) is the primary governance and decision-making body for FedRAMP and its members are Chief Information Officers from across the Government, including the DoD. Federal agencies must use commercial CSOs that are FedRAMP authorized.[6] Once FedRAMP grants a commercial CSO a FedRAMP authorization, the authorization package is available to all Federal agencies to review and leverage when managing risks associated with introducing that authorized commercial CSO into their agency's operating environment.

*(U) FedRAMP is a government-wide program that standardizes the security assessment, authorization, and continuous monitoring process for cloud products and services.*

(U) To obtain a FedRAMP authorization, CSPs must implement baseline security controls in accordance with the NIST Risk Management Framework (RMF).[7] The NIST RMF is a step-by-step, risk-based approach to identify the security controls and standards needed to protect Government systems, networks, and data. CSPs are responsible for selecting the appropriate impact level for their commercial

[4] (U) OMB Memorandum, "Security Authorization of Information Systems In Cloud Computing Environments," December 8, 2011.

[5] (U) NIST defines Information Security Continuous Monitoring as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

[6] (U) FedRAMP considers its authorizations as "provisional" because CSPs must demonstrate that the commercial CSO initially meets the minimal security requirements and maintains the same level of security through annual reassessments and its continuous monitoring process. The DoD also has a similar authorization process for commercial CSOs. Therefore, we refer to both the FedRAMP and DoD's provisional authorizations as "authorizations" for the purposes of this report.

[7] (U) NIST Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations," Revision 2, December 2018.

(U) CSO, which is validated through the FedRAMP authorization process. The level of risk or impact level is based on the sensitivity of the information expected to be stored and processed in the authorized commercial CSO. The impact level is based on the potential impact that certain events would have on an organization's ability to accomplish its assigned mission and protect its assets. FedRAMP categorizes commercial CSOs by the following three impact levels.

- **(U) High Impact level**. The loss of data confidentiality, integrity, or availability could have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Usually involves law enforcement, emergency services, financial, or health systems.
- **(U) Moderate Impact level**. The loss of data confidentiality, integrity, or availability could result in serious adverse effects on an agency's operations, assets, or individuals. Serious adverse effects could include significant operational damage to agency assets or financial loss.
- **(U) Low Impact level**. The loss of data confidentiality, integrity, or availability could result in limited adverse effects on an agency's operations, assets, or individuals.[8]

(U) To retain a FedRAMP authorization, commercial CSOs must maintain an adequate security posture to demonstrate that system security is operating as intended. FedRAMP requires that authorized commercial CSOs have a continuous monitoring capability and undergo an annual review by a Third-party Assessment Organization (3PAO). The 3PAOs evaluate the CSPs' implementation of, and compliance with, baseline security controls. The 3PAO issues an annual report identifying the commercial CSO's risks, which FedRAMP uses as part of its reassessment of the commercial CSO's authorization. The CSP's continuous monitoring activities should include the mitigation of open Plan of Action and Milestones (POA&M) items and managing significant changes or critical vulnerabilities for the authorized commercial CSO, which is tracked in monthly continuous monitoring reports.

*(U) To retain a FedRAMP authorization, commercial CSOs must maintain an adequate security posture to demonstrate that system security is operating as intended.*

[8] (U) According to FedRAMP, as of November 2017 the DoD accounted for 33 percent of high impact level services used by the Government. FedRAMP introduced their High Baseline to account for the Government's most sensitive unclassified data in cloud computing environments, including data that involves the protection of life and prevents financial ruin.

(U) The JAB then reviews the 3PAO reports and the CSPs' continuous monitoring documentation for each authorized commercial CSO and, if it identifies a deficiency, the JAB may take one or more of the following actions.

- **(U) Detailed Finding Review**. Based on the JAB's review, it may request that the CSP assess the authorized commercial CSO's deficiency and report the cause and remedy to the Board.
- **(U) Corrective Action Plan**. If the deficiency is not resolved, the JAB then requests that the CSP perform a root-cause analysis and provide a formal plan for remediation to the Board.
- **(U) Suspension**. If the deficiency is still not resolved, the JAB temporarily suspends a commercial CSO's authorization until the CSP can resolve the identified deficiency.
- **(U) Revocation**. If the deficiency cannot be resolved, the JAB permanently revokes the commercial CSO's authorization, which means that the CSP must restart the authorization process if seeking re-authorization.

(U) Additionally, the JAB requires agency authorizing officials (AOs) to oversee the CSPs' continuous monitoring activities on behalf of their agency. AOs are Government officials who are delegated the responsibility for information systems and authorizing their systems to ensure the level of risk is acceptable to support mission requirements, including the use of commercial CSOs. FedRAMP requires agency AOs to review and consider all documentation related to continuous monitoring activities, including 3PAO reports, the CSPs' POA&M report, and monthly continuous monitoring reports.[9] These reviews assist AOs with risk-based decisions for using an authorized commercial CSO.

> *(U) AOs review and consider all documentation related to continuous monitoring activities, including 3PAO reports, the CSPs' POA&M report, and monthly continuous monitoring reports.*

[9] (U) A POA&M is a document used to record known weaknesses and risks to a system or network, the actions and resources needed to mitigate those weaknesses, and the expected milestones for mitigating the weaknesses.

## (U) DoD Requirements for Cloud Security

(U) DoD Instruction 8500.01 requires DoD Component heads to comply with applicable security technical implementation guides, security configuration guides, and the DoD Cloud Computing Security Requirements Guide (SRG).[10] DoD Instruction 8500.01 also requires that DoD Component Chief Information Officers (CIOs), on behalf of their DoD Component heads, develop, implement, maintain, and enforce a DoD Component cybersecurity program that is consistent with the DoD cybersecurity program.

(U) The DoD Cloud Computing SRG requires completion of a two-step process before DoD Components can use commercial CSOs. First, DoD Components must select a commercial CSO that has a DoD authorization from the Defense Information Systems Agency (DISA) at the appropriate DoD impact level.[11] Second, DoD Components must grant a system-level authorization to operate (ATO) when using an authorized commercial CSO. The DoD Cloud Computing SRG also requires DoD Components and AOs to follow the DoD RMF process outlined in DoD Instruction 8510.01 for understanding the risk of using a commercial CSO and accepting that risk through an ATO.[12]

*(U) The DoD Cloud Computing SRG requires completion of a two-step process before DoD Components can use commercial CSOs.*

(U) After receiving a DoD authorization and a DoD Component ATO, CSPs must maintain an acceptable security posture for the authorized commercial CSO through continuous monitoring activities such as periodic vulnerability scans, 3PAO annual assessments, and effective implementation of security controls, as required by the DoD Cloud Computing SRG.[13] As part of the DoD authorization process, the DoD Cloud Computing SRG requires that DISA implement a continuous monitoring capability, similar to FedRAMP, for reviewing the documentation supporting continuous monitoring activities by the CSP to mitigate vulnerabilities and address risks identified in POA&Ms. Furthermore, DISA takes similar actions as FedRAMP to hold CSPs accountable when they fail to maintain an adequate continuous monitoring capability.

[10] (U) DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014 (Incorporating Change 1, October 7, 2019); and DISA, “DoD Cloud Computing Security Requirements Guide,” Version 1, Release 3, March 6, 2017. During the audit, DISA updated the Guide (Version 1, Release 4) on January 14, 2022.

[11] (U) A DoD Component may use a non-DoD approved CSO if it has a validated mission requirement that only that specific CSP’s CSO can fulfill. To use a non-DoD approved CSO, DoD Components must obtain a waiver from the DoD CIO.

[12] (U) DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014 (Incorporating Change 3, December 29, 2020).

[13] (U) NIST 800-53 defines a vulnerability as a weakness in an information system, system security procedures, or internal controls that could be exploited by malicious actors.

## (U) DoD Authorization Processes

(U) For the first step of using commercial CSOs, the DoD Cloud Computing SRG requires that DoD Components select a commercial CSO that has a DoD authorization at the appropriate DoD impact level. DISA performs the DoD authorization process, which assesses the risk to the DoD when approving commercial CSOs to connect to the DoD Information Networks but does not fully address the mission risk.[14]

*(U) DISA performs the DoD authorization process, which assesses the risk to the DoD when approving commercial CSOs to connect to the DoD Information Networks.*

(U) The DoD authorization process expands on the FedRAMP authorization process by requiring the CSP to implement up to 47 additional NIST RMF controls based on risks specific to DoD-defined impact levels for storing and processing information. The DoD impact levels range from the lowest at level 2 to the highest at level 6.

(U) The DoD Cloud Computing SRG requires DISA to take the following actions when granting a DoD authorization to a commercial CSO.

- (U) Verify whether the CSP implemented the additional NIST RMF security controls for the authorized commercial CSO required by the DoD impact level.
- (U) Review annual 3PAO assessment reports to identify the authorized commercial CSO's risks and vulnerabilities.
- (U) Review the CSP's annual continuous monitoring reporting to ensure that the authorized commercial CSO complies with FedRAMP and DoD security requirements.
- (U) Verify that the CSP took the necessary corrective actions to mitigate the authorized commercial CSO's security risks or findings identified in annual 3PAO, POA&M, and monthly continuous monitoring reports.

[14] (U) The DoD Information Networks are a globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to Service members, policy makers, and support personnel.

## *(U) DoD Component ATO Process*

(U) For the second step of using an authorized commercial CSO, the DoD Cloud Computing SRG requires DoD Component AOs to grant a system-level ATO, including reviewing supporting documentation, when using an authorized commercial CSO. The DoD Cloud Computing SRG requires that AOs assess the overall risk of introducing the authorized commercial CSO into their agency's operating environment as part of the ATO process. The AOs' assessment depends on the type of CSO service (Software, Platform, or Infrastructure as a Service) and the impact level. After granting a system-level ATO, AOs must review and consider documentation supporting continuous monitoring activities on a periodic basis to ensure that commercial CSOs maintained an acceptable security posture.

*(U) The DoD Cloud Computing SRG requires DoD Component AOs to grant a system-level ATO, including reviewing supporting documentation, when using an authorized commercial CSO.*

(U) To understand the overall or residual risk (that is, the portion of risk remaining after implementing security measures) of using an authorized commercial CSO, AOs must review and leverage the supporting documentation for the FedRAMP and DoD authorizations and the commercial CSPs' continuous monitoring activities. The DoD Cloud Computing SRG does not require AOs to reassess the FedRAMP and DISA authorization processes; instead, AOs should leverage the results from the FedRAMP and DISA authorization processes while considering the risks identified. This review provides the AOs an understanding of the effectiveness of the controls, the risk associated with using that specific type of authorized commercial CSO in the DoD Component's operating environment, and whether the CSP needs to implement additional security controls to reduce risk to an acceptable level. Examples of FedRAMP continuous monitoring documentation that AOs should review include the annual 3PAO reports, POA&Ms reports, and monthly continuous monitoring reports.

## *(U) DoD Cloud Systems Reviewed*

(U) We nonstatistically selected five cloud systems for review from the Army, Navy, Air Force, and Marine Corps. The DoD Components used three different authorized commercial CSOs for the five systems reviewed. The three authorized commercial CSOs used represented two of the four DoD-defined impact levels, and two of the

(U) three types of cloud services as defined by NIST. Table 1 provides the names and descriptions of the five cloud systems reviewed, the DoD impact level, and the names and type of authorized commercial CSOs used by the DoD Components.

*(U) Table 1. DoD Component Cloud Systems Reviewed, System Descriptions, and CSOs Used*

| (~~CUI~~)<br>**DoD Component** | **DoD Component System** | **Impact Level*** | **Type of Cloud Service Offering** | **Cloud System Description** |
|---|---|---|---|---|
| Army | DoD Explosives Safety Knowledge Enterprise System | (~~CUI~~) [redacted] | Infrastructure as a Service | (~~CUI~~) [redacted] |
| Navy | Navy Enterprise Resource Planning | (~~CUI~~) [redacted] | Infrastructure as a Service | (~~CUI~~) [redacted] |
| Air Force | Tailored Multitenancy Integrated Service | (~~CUI~~) [redacted] | Infrastructure as a Service | (~~CUI~~) [redacted] |
| Air Force | Cloud One | (~~CUI~~) [redacted] | Infrastructure as a Service and Platform as a Service | (~~CUI~~) [redacted] |
| Marine Corps | MarineNet | (~~CUI~~) [redacted] | Infrastructure as a Service | (~~CUI~~) [redacted]<br>**(~~CUI~~)** |

* (U) The DoD Cloud Computing SRG defines impact level 4 as a commercial CSO that can store and process controlled unclassified information and impact level 5 as a commercial CSO that can support unclassified national security systems.

(U) Source: The DoD OIG.

## (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.[15] We identified internal control weaknesses related to DoD Component AOs not reviewing all required documentation to assess risks associated with using authorized commercial CSOs when granting and maintaining ATOs as required by Federal and DoD guidance. We will provide a copy of the report to the senior officials responsible for internal controls in the DoD CIO, Army, Navy, Air Force, Marine Corps, and DISA.

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

# (U) Finding

## (U) DoD Components Used Authorized Commercial CSOs But Did Not Review All Required Documentation to Consider Risks When Granting and Maintaining ATOs

(U) The Army, Navy, Air Force, and Marine Corps used three commercial CSOs that were FedRAMP and DoD authorized and at the appropriate DoD impact level for the five systems reviewed. However, the AOs did not review all required documentation to consider the authorized commercial CSOs' risks to their systems when granting and reassessing the ATOs on a periodic basis thereafter. Periodic assessments seek to ensure that the CSPs maintained an acceptable security posture as required by Federal and DoD security requirements. Specifically, the AOs did not consider risks to specific systems that were identified in the supporting documentation; such as annual 3PAO, POA&M, and monthly continuous monitoring reports; for the authorized commercial CSOs' FedRAMP and DoD authorization process and continuous monitoring activities, as applicable to the type and impact level of the CSO.

(U) The AOs did not review all required documentation to consider the authorized commercial CSOs' risks when granting and maintaining ATOs because all five AOs believed that the FedRAMP and DoD authorization process was sufficient to mitigate risks to their respective systems.

(~~CUI~~) Unless AOs review all required documentation to consider the risks to their respective systems, DoD Components may be unaware of vulnerabilities and cybersecurity risks associated with operating their systems or storing their data in the authorized commercial CSOs. For example, if AOs reviewed POA&M reports for the authorized commercial CSOs, they would be aware of the open vulnerabilities. We determined that the three authorized commercial CSOs used by the DoD Components had a combined [redacted] significant unmitigated vulnerabilities, [redacted]. We also determined that two of the three authorized commercial CSOs used had a combined [redacted] unmitigated vulnerabilities [redacted].[16] These vulnerabilities could allow malicious actors to [redacted]

[16] (~~CUI~~) [redacted]

(~~CUI~~) [redacted].[17] By using authorized commercial CSOs with those types of unmitigated vulnerabilities, the DoD may be at an increased risk of successful cyber attacks, system and data breaches, data loss and manipulation, or unauthorized disclosures of mission-essential or sensitive information.

## (U) DoD Components Did Not Follow Federal and DoD Guidance When Granting and Maintaining ATOs

(U) The Army, Navy, Air Force, and Marine Corps used commercial CSOs that were FedRAMP and DoD authorized and at the DoD-appropriate impact level, but did not review all required documentation to consider the authorized commercial CSOs' risks to their respective systems before granting and reassessing the ATOs on a periodic basis thereafter, as required by Federal and DoD security requirements.

*(U) AOs also did not review documentation supporting the continuous monitoring activities, such as annual 3PAO, POA&M, and monthly continuous monitoring reports on a periodic basis.*

(U) Before granting an ATO, AOs must understand the overall security posture of the authorized commercial CSO by reviewing the system security plan, including known cybersecurity risks and the security controls in place to mitigate them, and the results of annual 3PAO assessments and other continuous monitoring activities as they apply to the type and impact level of the CSO used. These actions, when taken, allow AOs to determine whether CSPs took the necessary actions to mitigate identified vulnerabilities to an acceptable level of risk for the data stored and processed within the authorized commercial CSO. Based on those reviews, DoD Components either need to implement additional security controls to mitigate residual risk to an acceptable level or require CSPs to implement additional security requirements to reduce the level of risk. If the CSPs mitigation is still not sufficient, DoD Components should then define additional security requirements tailored for the authorized commercial CSO in the contract or service agreements according to the DoD Cloud Computing SRG. However, the AOs relied on FedRAMP and DoD authorization and continuous monitoring processes without reviewing and considering the risks identified by those processes to fully understand the overall cybersecurity posture of the authorized commercial CSOs. Specifically, the AOs did not review the authorized commercial CSOs' documentation supporting the FedRAMP and DoD authorizations. The AOs also did not review documentation supporting the continuous monitoring activities,

[17] (~~CUI~~) [redacted]

(U) such as annual 3PAO, POA&M, and monthly continuous monitoring reports on a periodic basis to ensure that the CSOs maintained an acceptable security posture as required by the DoD Cloud Computing SRG.

(U) Had the AOs reviewed the documentation supporting the FedRAMP and DoD authorization processes and continuous monitoring activities, it would have provided them with a better understanding of the security posture of the authorized commercial CSOs and awareness of the types and number of vulnerabilities (risks) associated with each authorized commercial CSO. By not considering all the required documentation to assess the identified risks and ensure that the authorized commercial CSOs maintained an acceptable security posture, AOs were not aware of the overall risk of using the authorized commercial CSO; thereby making their DoD Components more susceptible to malicious actors exploiting cybersecurity vulnerabilities. Therefore, the CIOs for the Army, Navy, and Air Force should require the AOs to reevaluate the ATOs for the five cloud systems we reviewed, including a review of all required documentation to consider the risks associated with using the authorized commercial CSOs, such as the documentation supporting the FedRAMP and DoD authorization processes and continuous monitoring activities, as required by the DoD Cloud Computing SRG.[18]

## (U) AOs Relied on the FedRAMP and DoD Authorization Processes Instead of Reviewing All Required Documentation to Consider CSOs' Risks

(U) For the five cloud systems reviewed, AOs for the Army, Navy, Air Force, and Marine Corps did not review all required documentation to consider the risks to their respective systems before granting and when maintaining ATOs because they believed that the FedRAMP and DoD authorization and continuous monitoring processes were sufficient to mitigate risks. Specifically, the DoD Component AOs focused on internal network and system-specific risks, such as the vulnerabilities identified by network security alerts and internal system scans, without reviewing documentation that identified the commercial CSOs' risks before granting an ATO.

(U) By only reviewing internal network and system-specific risks, AOs have reduced awareness of the authorized commercial CSOs' vulnerabilities or risks that could impact their DoD Component's overall cybersecurity posture, network,

*(U) AOs have reduced awareness of the authorized commercial CSOs' vulnerabilities or risks that could impact their DoD Component's overall cybersecurity posture, network, or mission.*

[18] (U) The Department of the Navy Deputy CIO for the Marine Corps reports to the Department of the Navy CIO; therefore, we will direct any recommendations for the Marine Corps to the Department of the Navy CIO.

(U) or mission.  For example, AOs would not be aware of systemic risks, such as the vulnerabilities that we identified with the authorized commercial CSOs used by the DoD Components that could allow malicious actors to exploit or circumvent user authentication, elevate user privileges, or make system configuration changes. Without awareness of the authorized commercial CSOs' systemic risks, AOs would also not be able to implement any additional controls needed to reduce the overall risks associated with using the authorized commercial CSOs.  See Table 2 for each DoD Component AO's explanation for not reviewing all required documentation to consider the commercial CSOs risks as required.

*(U) Table 2.  DoD Component AOs' Explanations for Not Reviewing All Required Documentation to Consider Authorized Commercial CSOs' Risks*

| **(U)**<br>**DoD Component** | **DoD Component System** | **Considered Overall Risks or Had Evidence of Review** | **DoD Component AOs' Explanation for Not Reviewing All Required Documentation** |
|---|---|---|---|
| Army | DoD Explosives Safety Knowledge Enterprise System | No | The AO was not aware of the requirement to consider the CSO-level risks and believed that it was not necessary to review information from the FedRAMP and DoD authorizations because those risks were previously considered during the respective authorization processes. |
| Navy | Navy Enterprise Resource Planning | No | The AO relied on internal system scans and the FedRAMP and DoD authorization processes without reviewing the supporting documentation.  Although the AO reviewed these scans, the AO would not be aware of the authorized commercial CSO's risks. |
| Air Force | Tailored Multitenancy Integrated Service | No | The AO reviewed the risks identified in the FedRAMP and DoD authorizations for the authorized commercial CSO when granting the initial ATO, but could not provide evidence of their review.  In addition, the AO did not review the authorized commercial CSO's documentation supporting the continuous monitoring activities thereafter. |
| Air Force | Cloud One | No | The AO relied on internal system scans to assess risks after granting an ATO.  Although the AO reviewed these scans, the AO would not be aware of the authorized commercial CSO's risks.<br>**(U)** |

*(U) Table 2. DoD Component AOs' Explanations for Not Reviewing All Required Documentation to Consider Authorized Commercial CSOs' Risks (cont'd)*

| (U)<br>DoD Component | DoD Component System | Considered Overall Risks or Had Evidence of Review | DoD Component AOs' Explanation for Not Reviewing All Required Documentation |
|---|---|---|---|
| Marine Corps | MarineNet | No | The AO did not request the documentation supporting the FedRAMP and DoD authorization processes and the continuous monitoring activities for the authorized commercial CSO.<br>**(U)** |

(U) Source: The DoD OIG.

(U) Although we reviewed only five cloud systems used by DoD Components, we identified that none of the AOs reviewed the required documentation to consider the authorized commercial CSOs' risks before granting ATOs and reassessing the ATO on a periodic basis thereafter, which leads us to believe this could be a systemic problem within the DoD. The DoD Cloud Computing SRG requires that DoD Component AOs review all required documentation supporting the commercial CSOs' authorization process and continuous monitoring activities to consider CSOs' risks to their respective systems and follow the normal DoD RMF process when granting and maintaining ATOs.

(U) Additionally, DoD Instruction 8500.01 requires that the DoD CIO monitor, evaluate, and provide advice to the Secretary of Defense regarding all DoD cybersecurity activities and oversee implementation of DoD cybersecurity policy and guidance consistent with this instruction and in accordance with applicable Federal law and regulations. DoD Instruction 8500.01 also requires DoD Component heads to ensure that all DoD information technology under their purview complies with applicable security technical implementation guides, security configuration guides, and SRGs. DoD Instruction 8500.01 further requires that DoD Component CIOs, on behalf of the respective DoD Component heads, develop, implement, maintain, and enforce a DoD Component cybersecurity program that is consistent with the DoD cybersecurity program, which includes following the DoD Cloud Computing SRG and the DoD RMF process for granting and maintaining ATOs for systems that use an authorized commercial CSO.

(U) Without reviewing all required documentation to consider the authorized commercial CSOs' risks to their respective systems, DoD Component AOs were not making fully informed decisions when granting and maintaining ATOs, and increasing the risks to their systems and networks.  Therefore, the DoD CIO should emphasize the importance of following the DoD Cloud Computing SRG when using commercial CSOs and reviewing all required documentation to consider the CSOs' risks before granting and when maintaining system-level ATOs, which should be documented as part of the ATO process.

*(U) DoD Component AOs were not making fully informed decisions when granting and maintaining ATOs, and increasing the risks to their systems and networks.*

## (U) The DoD May be at an Increased Risk of Successful Cybersecurity Attacks

(U) The DoD continues to face sophisticated and evolving cyber attacks from malicious actors that constantly attempt to gain access to DoD systems and sensitive data, and exploit cybersecurity vulnerabilities.  As part of the FedRAMP and DoD authorization processes, DISA is responsible for reviewing the authorized commercial CSOs' documentation supporting CSPs continuous monitoring activities to mitigate vulnerabilities.  Continuous monitoring activities are designed to ensure that the authorized commercial CSOs maintain an adequate security posture by demonstrating that security controls are operating as intended when hosting DoD systems or data.

(~~CUI~~) However, the POA&Ms for the three authorized commercial CSOs we reviewed included a number of open [redacted] vulnerabilities, [redacted] that AOs should have been aware of and considered when making decisions to grant or continue system-level ATOs.  AOs play a vital role in supporting the DoD's efforts to manage risk to the DoD Information Network when granting ATOs.  However, if AOs do not review all required documentation when considering the authorized commercial CSOs' risks to their respective systems before granting and periodically reassessing the ATO thereafter, DoD Components may be unaware of known vulnerabilities and cybersecurity risks associated with operating their systems or storing their data in authorized commercial CSOs.

*(U) DoD Components may be unaware of known vulnerabilities and cybersecurity risks associated with operating their systems or storing their data in authorized commercial CSOs.*

(~~CUI~~) For the five systems in our audit scope, we reviewed annual 3PAO reports from 2019 through 2021, POA&M reports from November 2021, and monthly continuous monitoring reports from May 2021 through October 2021 for the three authorized commercial CSOs used. Based on the unmitigated vulnerabilities from the November 2021 POA&M reports, we determined that the three authorized commercial CSOs had a combined [redacted] significant unmitigated vulnerabilities—[redacted]—[redacted].[19] Specifically, the three authorized commercial CSOs used had the following significant unmitigated vulnerabilities.

- (~~CUI~~) [redacted]
- (~~CUI~~) [redacted]
- (~~CUI~~) [redacted]

(~~CUI~~) Additionally, we reviewed the combined [redacted] unmitigated [redacted] vulnerabilities from the POA&M reports for the three authorized commercial CSOs [redacted] [redacted]

(~~CUI~~) As of June 2022, we determined that two of the three authorized commercial CSOs had a combined [redacted] unmitigated [redacted] vulnerabilities [redacted]

[19] (~~CUI~~) [redacted]

(~~CUI~~) [redacted][20] [redacted]

*(~~CUI~~)* [redacted]

(~~CUI~~) By using authorized commercial CSOs with unmitigated [redacted] vulnerabilities [redacted], the DoD unnecessarily increases its risk of successful cyber attacks, system and data breaches, data loss and manipulation, or unauthorized disclosures of mission-essential or sensitive information. Therefore, the DISA Director, through the agency Risk Management Executive, should coordinate with the JAB for FedRAMP or the cognizant Federal agency to require that commercial CSPs remediate all vulnerabilities [redacted] or provide documentation that describes why the risk of mission impact is low, along with the planned actions and milestones to address or remediate the vulnerabilities.

## (U) Other Matters of Interest

(U) Army, Navy, Air Force, and Marine Corps contracting officials did not always include the required Defense Federal Acquisition Regulation Supplement (DFARS) cloud computing clauses in the contracts for the five cloud systems reviewed.

*(U) Of the five contracts reviewed, three contracts included the necessary contract clauses, but the remaining two contracts did not.*

Of the five contracts reviewed, three contracts included the necessary contract clauses, but the remaining two contracts did not. The DoD Cloud Computing SRG requires contracting officials to comply with DFARS 239.76

[20] (~~CUI~~) [redacted]

(U) by including DFARS clauses 252.204-7012 and 252.239-7010 in all cloud service contracts unless granted a waiver by the DoD CIO. The DFARS clauses require that the CSP and the authorized commercial CSO must have a DoD authorization at the appropriate impact level before contract award unless granted a waiver, and that the CSP must report all cyber incidents.

(U) Army contracting officials did not include either of the required DFARS cloud computing clauses in the contract for the DoD Explosives Safety Knowledge Enterprise System when it transitioned from the Space and Naval Warfare Systems Command to the General Services Administration. During the audit, we notified the Army of the missing clauses and the contracting officer modified the contract to include them. Therefore, we did not include a recommendation to the Army for corrective action in this report related to the DFARS clauses.

(U) Air Force contracting officials did not include either of the required DFARS cloud computing clauses in the contract for the Tailored Multitenancy Integrated Service system because they awarded the contract in September 2015, which was before the issuance of the DoD Cloud Computing SRG. During the audit, we notified the Air Force about the missing clauses and the contracting officer modified the contract to include them. Therefore, we did not include a recommendation to the Air Force for corrective action in this report related to the DFARS clauses.

## (U) Unsolicited Management Comments

(U) A summary of unsolicited management comments on the background, finding, and recommendations, and our response, is in Appendix B.

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

### *(U) Revised Recommendations*

(~~CUI~~) As a result of management comments, we revised Recommendations 2.a and 2.b to correct the titles for the Department of the Navy CIO and the Navy and Marine Corps Deputy CIOs. We also revised Recommendation 5 to clarify the DISA Risk Management Executive's responsibilities in the DoD authorization process for commercial CSOs and identify documentation required when vulnerabilities [redacted].

## (U) Recommendation 1

**(U) We recommend that the Chief Information Officer for the Army require the authorizing official for the DoD Explosives Safety Knowledge Enterprise System to reevaluate the authorization to operate, including a review of all required documentation to consider the risks associated with using the authorized commercial cloud service offering, such as the documentation supporting the Federal Risk and Authorization Management Program and the DoD authorization processes and the continuous monitoring activities, as required by the DoD Cloud Computing Security Requirements Guide.**

### *(U) Chief Information Officer for the Army Comments*

(U) The Army CIO agreed, stating that the Army has taken steps to effectively manage its cybersecurity posture of all systems, including those hosted in a cloud environment. The Army CIO stated that the AO for the DoD Explosives Safety Knowledge Enterprise System would review the ATO and all supporting documentation to ensure that the system complies with Federal, DoD, and Army guidance, including the DoD Cloud Computing SRG. The Army CIO stated that the AO would complete the review by April 30, 2023.

### *(U) Our Response*

(U) Comments from the Army CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Army CIO provides documentation demonstrating that the AO for the DoD Explosives Safety Knowledge Enterprise System reviewed all required documentation to maintain the ATO and considered the risks associated with using the authorized commercial CSO, as required by the DoD Cloud Computing SRG.

## (U) Recommendation 2

**(U) We recommend that the Department of the Navy Chief Information Officer:**

a. **(U) Require that the authorizing official for the Navy Enterprise Resource Planning system, in coordination with the Department of the Navy Deputy Chief Information Officer for the Navy, reevaluate the authorization to operate, including a review of all required documentation to consider the risks associated with using the authorized commercial cloud service offering, such as the documentation supporting the Federal Risk and Authorization Management Program and the DoD authorization processes and continuous monitoring activities, as required by the DoD Cloud Computing Security Requirements Guide.**

b. **(U) Require that the authorizing official for the MarineNet system, in coordination with the Department of the Navy Deputy Chief Information Officer for the Marine Corps, reevaluate the authorization to operate, including a review of all required documentation to consider the risks associated with using the authorized commercial cloud service offering, such as the documentation supporting the Federal Risk and Authorization Management Program and the DoD authorization processes and continuous monitoring activities, as required by the DoD Cloud Computing Security Requirements Guide.**

### *(U) Department of the Navy Chief Information Officer Comments*

(U) The Department of the Navy CIO agreed, stating that the Navy and Marine Corps AOs needed to improve their access to, and review of, risk documentation supporting the FedRAMP and the DoD authorization processes and continuous monitoring activities, as required by the DoD Cloud Computing SRG. However, the Department of the Navy CIO disagreed that the AO for the Navy Enterprise Resource Planning system needed to specifically reevaluate the system's ATO because that action would be a function of reviewing the FedRAMP and DoD risk documentation and the Navy's continuous monitoring activities. The Department of the Navy CIO stated that the Marine Corps had begun implementing changes in its processes for Marine Corps AO documentation reviews.

### *(U) Our Response*

(U) Although the Department of the Navy CIO disagreed with reevaluating the ATO for the Navy Enterprise Resource Planning system, the Department of the Navy CIO's plan to review the risk documentation supporting the FedRAMP and DoD authorization processes as part of the continuous monitoring activities for the Navy and Marine Corps systems meets the intent of the recommendations. Therefore, the recommendations are resolved but open. We will close the recommendations once the Department of the Navy CIO provides documentation demonstrating that the AOs for the Navy Enterprise Resource Planning and MarineNet systems reviewed the risk documentation support for the FedRAMP and DoD authorization and considered the identified risks as part of each system's continuous monitoring activities.

## (U) Recommendation 3

**(U) We recommend that the Chief Information Officer for the Air Force require that the authorizing officials for the Tailored Multitenancy Integrated Service and Cloud One systems reevaluate the authorizations to operate, including a review of all required documentation to consider the risks associated with using the authorized commercial cloud service offering, such as the documentation supporting the Federal Risk and Authorization Management Program and DoD authorization processed and continuous monitoring activities, as required by the DoD Cloud Computing Security Requirements Guide.**

### *(U) Department of the Air Force Comments*

(U) The Air Force Deputy CIO, responding for the Air Force CIO, partially agreed, stating that the Air Force Chief Information Security Officer would review and update guidance to ensure Air Force AOs consider and review risk assessment documentation when using authorized commercial CSOs. In addition, the Deputy CIO stated that the Chief Information Security Officer would review and update the Department of the Air Force Organizational Risk Tolerance Baseline and Information Security Continuous Monitoring Strategy to include unique requirements for using authorized commercial CSOs. The Deputy CIO stated that the Chief Information Security Officer would complete the reviews and updates by September 30, 2023.

### *(U) Our Response*

(U) Comments from the Air Force Deputy CIO partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. The Air Force Deputy CIO agreed to review and update Air Force guidance; however, he did not specifically address whether the AOs would reevaluate the ATOs for the Tailored Multitenancy Integrated Service and Cloud One systems. Therefore, we request that the Air Force CIO provide additional comments within 30 days in response to the final report that describe the Air Force's planned actions to reevaluate the ATOs, including the risks identified by the FedRAMP and DoD authorization processes, as required by the DoD Cloud Computing SRG, for the two commercial CSOs that we reviewed.

## *(U) Recommendation 4*

**(U) We recommend that the DoD Chief Information Officer emphasize the importance of following the DoD Cloud Computing Requirements Guide when using commercial cloud service offerings, and reviewing all required documentation to consider the commercial cloud service offering's risks before granting and when maintaining system-level authorizations to operate, which should be documented as part of the authorization to operate process.**

### *(U) DoD Chief Information Officer Comments*

(U) The DoD CIO agreed, reiterating the importance of the DoD Cloud Computing SRG and stating that the guide's requirements have been established as a regulatory requirement in the DFARS clauses for all DoD cloud contracts. The DoD CIO stated that the DoD Components should use DoD tools to access cloud security-related documentation and ensure their cloud security processes comply with the DoD Cloud Computing SRG. In addition, the DoD CIO requested that we consider the implementation of the DFARS clauses as action to close this recommendation.

### *(U) Our Response*

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. Although the DFARS clauses address commercial CSPs' compliance with the DoD guidance, they do not address the DoD Component AOs' compliance with the Cloud Computing SRG. Therefore, we will close the recommendation once the DoD CIO provides documentation of the actions taken to emphasize the importance of DoD Component AOs following the DoD Cloud Computing SRG and reviewing all required documentation to consider the risks of using authorized commercial CSOs before granting and when maintaining system-level ATOs.

## *(U) Recommendation 5*

**(~~CUI~~) We recommend that the Defense Information Systems Agency Director, through the agency Risk Management Executive, coordinate with the Joint Authorization Board of the Federal Risk and Authorization Management Program to require that commercial cloud service providers remediate all vulnerabilities [redacted] or provide documentation that describes why the risk of mission impact is low, along with the planned actions and milestones to address or remediate the vulnerabilities.**

## *(U) Defense Information Systems Agency Comments*

(~~CUI~~) The DISA CIO, responding for the DISA Director, partially agreed, stating that vulnerabilities [redacted] did not always present a risk to the CSO or DoD data. The DISA CIO stated that identified vulnerabilities must be analyzed to determine the appropriate level of risk and based on risk level, mitigated within FedRAMP established timelines. Furthermore, the DISA CIO stated that the DISA would continue to collaborate, through its Risk Management Executive, with the FedRAMP JAB to address important security actions, [redacted] as required by Federal guidance.

## *(U) Our Response*

(~~CUI~~) Comments from the DISA CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DISA CIO provides documentation demonstrating that the CSPs either mitigated the vulnerabilities [redacted] or provided documentation supporting that the assessed vulnerabilities have a low risk to mission impact.

# (U) Appendix A

## (U) Scope and Methodology

(U) We conducted this performance audit from January 2020 through November 2022, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We interviewed officials from the DoD Office of the Chief Information Officer, DISA, Army, Navy, Air Force, and Marine Corps, and requested information to determine whether DoD Components complied with Federal and DoD security requirements when using commercial cloud computing. We nonstatistically selected five cloud systems for review from the Army, Navy, Air Force, and Marine Corps. The DoD Components used three different authorized commercial CSOs for the five systems reviewed. The three authorized commercial CSOs used represented two of the four DoD-defined impact levels, Level 4 and Level 5, and two of the three types of cloud services, Infrastructure as a Service and Platform as a Service, as defined by NIST.

(U) We reviewed FedRAMP, the DoD Cloud Computing SRG, DFARS, NIST, and other relevant DoD information technology policies and procedures to determine the security requirements and responsibilities for using authorized commercial CSOs. We reviewed relevant documentation accompanying the authorized commercial CSOs' FedRAMP and DoD authorizations and available continuous monitoring activities to determine whether the DoD Components granted and maintained system ATOs in accordance with DoD Cloud Computing SRG requirements.

(U) We interviewed DISA officials to identify and assess their process for approving commercial CSO authorizations and verifying the CSPs' compliance with Federal and DoD cloud computing security requirements. Specifically, we assessed whether DISA officials:

- (U) followed the DoD Cloud Computing SRG for granting a DoD authorization,
- (U) performed continuous monitoring of the CSPs' performance as required by the DoD Cloud Computing SRG, and

- (U) ensured that the CSPs resolved findings identified in annual 3PAO assessments and mitigated other vulnerabilities identified through CSP vulnerability scans and reporting, such as monthly continuous monitoring and POA&M reports.

(U) Additionally, we interviewed DoD Component officials from the Army, Navy, Air Force, and Marine Corps to identify how they reviewed and considered all required documentation to assess the risks of using an authorized commercial CSO when granting an ATO and on a periodic basis thereafter. Specifically, we:

- (U) determined whether AOs reviewed the FedRAMP and DISA documentation supporting authorization packages and continuous monitoring activities to determine whether the CSPs mitigated identified vulnerabilities;
- (U) requested documentation and interviewed DoD Component officials to determine their process for granting ATOs and continuous monitoring thereafter; and
- (U) reviewed contracts for each of the five systems reviewed to ensure that officials included the necessary clauses, defined security responsibilities, and outlined any additional security requirements as needed.

(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 comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

## (U) Internal Control Assessment and Compliance

(U) We reviewed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we reviewed DISA processes and controls in place for granting the commercial CSO's authorization. We also reviewed the DoD Component AOs' processes for granting and maintaining ATOs when using authorized commercial CSOs as required by the DoD Cloud Computing SRG. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

## (U) Use of Computer-Processed Data

(U) We used computer-processed data that we extracted from the DoD Information Technology Investment Portfolio and Select and Native Programming Data Input System to determine the universe of DoD cloud services.[21] However, we used only cloud service listing data from the DoD Information Technology Investment Portal to select a nonstatistical sample of cloud services for review. To assess the reliability of the data from the portal, we verified the accuracy of information with contractual and other source documentation available, such as task orders and security contract agreements. Therefore, we determined that the data was sufficiently reliable for the purpose of selecting a nonstatistical sample of cloud services to review for the audit.

(U) In addition, we used system-generated data from the DoD's Enterprise Mission Assurance Support Service system for the five systems reviewed to determine whether DoD Components used a DISA-approved commercial CSO before awarding a contract and granting an ATO for each selected commercial CSO. To ensure the accuracy of the information obtained, we compared information from the Enterprise Mission Assurance Support Service system with DISA and DoD Component source documentation such as the ATOs, system security plans, and security assessment reports. We determined that the data was sufficiently reliable for the purposes of the audit to determine whether the DoD Components reviewed and considered all risks to their respective systems when granting ATOs and reassessing risks on a periodic basis thereafter when using authorized commercial CSOs.

## (U) Prior Audit Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) and the Air Force Audit Agency (AFAA) issued four reports discussing cloud investments and cloud service requirements. Unrestricted GAO reports can be accessed at https://www.gao.gov/reports-testimonies. Unrestricted AFAA reports can be accessed at https://infolink.dodig.mil/portal/audit/afaa_reports/SitePages/Home.aspx by selecting the 'Audit Reports' check box.

[21] (U) The DoD Information Technology Investment Portal is the authoritative data source for DoD IT systems and aligns the information to the Defense IT Portfolio Registry. Select and Native Programming Data Input is the DoD authoritative database for the Department's Information Technology budget submission to the Office of Management and Budget and Congress.

## (U) GAO

(U) Report No. GAO-22-104070, "DoD Needs to Improve Workforce Planning and Software Application Modernization," June 29, 2022

> (U) In 2019, OMB updated its Federal Cloud Computing Strategy and established 14 key requirements for agencies to implement within three areas – security, procurement, and workforce. The GAO found that the DoD addressed 11 of the 14 OMB requirements, but gaps exist in its workforce planning. These workforce gaps included identifying future skills needed for cloud-based services, conducting regular evaluations of customer experiences and user needs, and developing and executing communication plans to inform employees of changes related to using these services. The GAO also found that although the DoD has established the scope for its rationalization efforts, its lacks established timeframes for completing the remaining activities and has not developed a long-term plan for its implementation with measurable objectives, milestones, and timelines. Additionally, the GAO identified weaknesses in the completeness of the DoD Components' cloud spending data, which could result in the underreporting of the DoD's cloud spending and incomplete information needed to make decisions on its information technology investments.

(U) Report No. GAO-20-126, "Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed," December 12, 2019

> (U) The GAO surveyed 24 Federal agencies and 47 CSPs to determine the extent to which they used FedRAMP to authorize cloud services and program participants identified FedRAMP benefits and challenges. The GAO found that, while the number of authorizations increased by 137 percent from June 2017 through July 2019, 15 agencies reported that they did not always use FedRAMP for authorizing cloud services and that they used 157 cloud services that were not authorized by the program. The OMB requires Federal agencies to use the program but did not effectively monitor compliance with this requirement and therefore, could not ensure that agencies met Federal security requirements.
>
> (U) Additionally, the GAO found that while program participants identified several benefits including the use of third-party assessors, program guidance, and standard security requirements, they also identified improvements for implementing FedRAMP, as shown by the following examples.
>
> - (U) Agencies reported that CSPs had difficulty implementing trusted Internet connections and were unable to comply with NIST encryption and multifactor authentication requirements.

- (U) Agencies also cited other areas that need improvement such as the authorization process, reviewing authorization packages, guidance for selecting cloud services, collaboration and coordination, clarity on the remedial action process, and time and resources to complete and maintain an agency authorization.

(U) Report No. GAO-19-58, "Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked," April 4, 2019

(U) The GAO reviewed 16 agencies' progress in implementing cloud services, the extent to which the agencies increased spending on cloud services and saved or avoided costs, and significant benefits the agencies identified in cloud investments. The GAO found that the DoD did not assess 237 of its 2,735 information technology investments to determine if they included cloud services. Although the DoD reported that investments using cloud services decreased from 2016 to 2019, DoD investment data for cloud services was incomplete because the DoD did not begin to track cloud spending until FY 2016 and misinterpreted the NIST definition of cloud computing. Furthermore, the DoD reported that its investment management system did not have the capability to track cloud savings and avoidance data. Even though DoD cloud investment data was incomplete, the DoD reported benefits from the acquisition of services such as improved customer service and strengthened mission assurance.

## *(U) AFAA*

(U) Report No. F2019-004-O10000, "Cloud Computing Security," March 28, 2019

(U) The AFAA found that Air Force personnel did not identify, prioritize, and monitor cloud migration or establish cloud service contract requirements in accordance with Federal guidance. Specifically, personnel from the Office of the Deputy Chief Information Officer of the Secretary of the Air Force did not identify and prioritize all systems and applications for cloud migration and monitor existing Air Force cloud migration efforts. In addition, Air Force personnel did not accurately define contract requirements or review and justify pass-through charges in accordance with the Federal Acquisition Regulation.

# (U) Appendix B

## (U) Unsolicited Management Comments and Our Response

(U) Although not required to comment, the DISA CIO provided comments on the Background, Finding, and Recommendations 1, 2, and 3. See the Management Comments section of the report for the full text of the DISA CIO's comments.

### *(U) Defense Information Systems Agency Comments on the Background*

(U) The DISA CIO stated that DoD Components are not required to select authorized commercial CSOs that have both a FedRAMP and DoD authorization. The DISA CIO stated that the DoD Cloud Computing SRG outlines several options for using an authorized commercial CSO depending on the DoD impact level supported and the DoD mission systems or applications hosted, which may or may not include leveraging the FedRAMP authorization.

### *(U) Our Response*

(U) Based on the DISA CIO's comments, we revised the report to clarify that DoD Components were not required to use an authorized commercial CSO that had a FedRAMP authorization. Although we acknowledge that there are several paths for DoD Components to use authorized commercial CSOs, the DoD Cloud Computing SRG encourages DoD Components to use commercial CSOs that have a FedRAMP authorization because DISA would have been involved in the validation and authorization activities.

### *(U) Defense Information Systems Agency Comments on the Finding*

(U) The DISA CIO stated that FedRAMP provides guidance for remediating vulnerabilities based on the risk environment. The DISA CIO stated that some vulnerabilities may exist for an extended period, but noted all vulnerabilities did not present an increased risk to the CSO or DoD data and could be mitigated through activities other than patching. Furthermore, the DISA CIO stated that FedRAMP and the DoD worked with commercial CSPs to address risks that are critical to DoD missions as part of the continuous monitoring process.

## *(U) Our Response*

(~~CUI~~) We acknowledge that instances may occur when vulnerabilities could continue to exist for an extended period without presenting increased risk. However, we identified unmitigated vulnerabilities for three commercial CSOs used by DoD Components that did not comply with timelines established by FedRAMP and the DoD Cloud Computing SRG, [redacted].

(U) Mitigating risks to DoD systems, networks, and data resulting from identified vulnerabilities is vital to maintaining a secure DoD information network. As previously stated, POA&Ms for the unmitigated vulnerabilities did not support that CSPs had reduced the risks for the aforementioned vulnerabilities to a low level of risk. Therefore, the DISA Risk Management Executive should continue to work with the commercial CSPs to ensure that they address identified vulnerabilities in a timely manner and provide documentation describing why the mission impact for vulnerabilities is low.

## *(U) Defense Information Systems Agency Comments on the Recommendations*

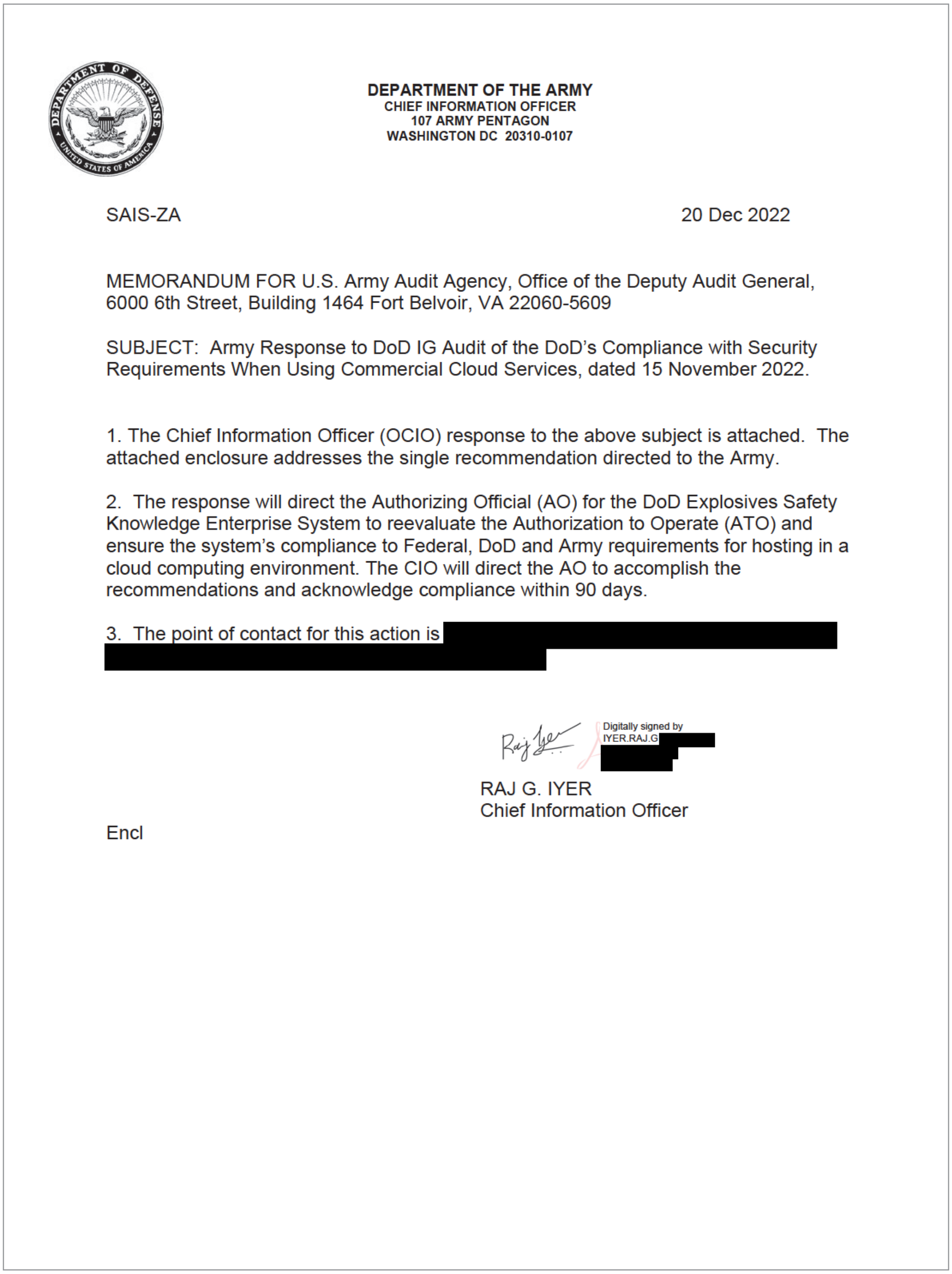
(U) The DISA CIO identified concerns with the wording of Recommendations 1, 2.a, 2.b, and 3, stating that the recommendations could be interpreted to require reassessments of the authorized commercial CSOs, which was contrary to the DoD's practice of "do once – reuse many" based on the FedRAMP and DoD authorization processes. The DISA CIO suggested that the DoD OIG revise the recommendations to require AOs to review the FedRAMP or DoD authorization documentation to identify potential risks that may impact the decision to deploy DoD systems or applications within authorized commercial CSOs.

## *(U) Our Response*

(U) We determined that AOs did not review all required documentation to consider the risks to their respective systems before granting and when maintaining ATOs because they believed that the FedRAMP and DoD authorization and continuous monitoring processes were sufficient to mitigate risks. The intent of Recommendations 1, 2.a, 2.b, and 3 was for AOs to review and consider all relevant risks based on documentation from the FedRAMP and DoD authorization processes and generated as part of their continuous monitoring activities, and not for them to conduct another ATO assessment. As such, we did not revise the recommendations.

# (U) Management Comments

## (U) Army Chief Information Officer



**DEPARTMENT OF THE ARMY**
**CHIEF INFORMATION OFFICER**
**107 ARMY PENTAGON**
**WASHINGTON DC 20310-0107**

SAIS-ZA 20 Dec 2022

MEMORANDUM FOR U.S. Army Audit Agency, Office of the Deputy Audit General, 6000 6th Street, Building 1464 Fort Belvoir, VA 22060-5609

SUBJECT: Army Response to DoD IG Audit of the DoD's Compliance with Security Requirements When Using Commercial Cloud Services, dated 15 November 2022.

1. The Chief Information Officer (OCIO) response to the above subject is attached. The attached enclosure addresses the single recommendation directed to the Army.

2. The response will direct the Authorizing Official (AO) for the DoD Explosives Safety Knowledge Enterprise System to reevaluate the Authorization to Operate (ATO) and ensure the system's compliance to Federal, DoD and Army requirements for hosting in a cloud computing environment. The CIO will direct the AO to accomplish the recommendations and acknowledge compliance within 90 days.

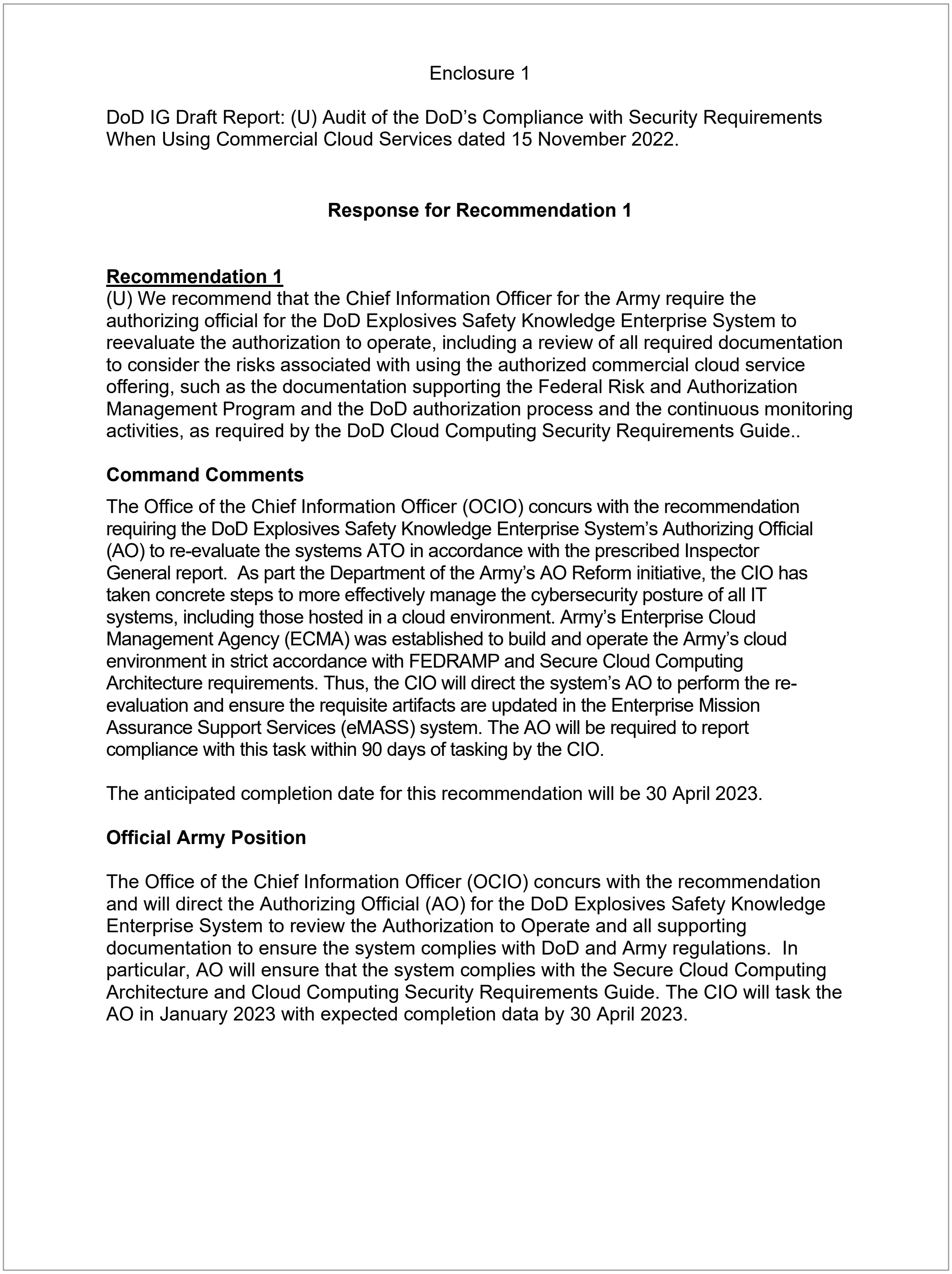
3. The point of contact for this action is [redacted]

Raj Iyer
Digitally signed by IYER.RAJ.G [redacted]

RAJ G. IYER
Chief Information Officer

Encl

# (U) Army Chief Information Officer (cont’d)



Enclosure 1

DoD IG Draft Report: (U) Audit of the DoD’s Compliance with Security Requirements When Using Commercial Cloud Services dated 15 November 2022.

**Response for Recommendation 1**

**Recommendation 1**

(U) We recommend that the Chief Information Officer for the Army require the authorizing official for the DoD Explosives Safety Knowledge Enterprise System to reevaluate the authorization to operate, including a review of all required documentation to consider the risks associated with using the authorized commercial cloud service offering, such as the documentation supporting the Federal Risk and Authorization Management Program and the DoD authorization process and the continuous monitoring activities, as required by the DoD Cloud Computing Security Requirements Guide..

**Command Comments**

The Office of the Chief Information Officer (OCIO) concurs with the recommendation requiring the DoD Explosives Safety Knowledge Enterprise System’s Authorizing Official (AO) to re-evaluate the systems ATO in accordance with the prescribed Inspector General report. As part the Department of the Army’s AO Reform initiative, the CIO has taken concrete steps to more effectively manage the cybersecurity posture of all IT systems, including those hosted in a cloud environment. Army’s Enterprise Cloud Management Agency (ECMA) was established to build and operate the Army’s cloud environment in strict accordance with FEDRAMP and Secure Cloud Computing Architecture requirements. Thus, the CIO will direct the system’s AO to perform the re-evaluation and ensure the requisite artifacts are updated in the Enterprise Mission Assurance Support Services (eMASS) system. The AO will be required to report compliance with this task within 90 days of tasking by the CIO.

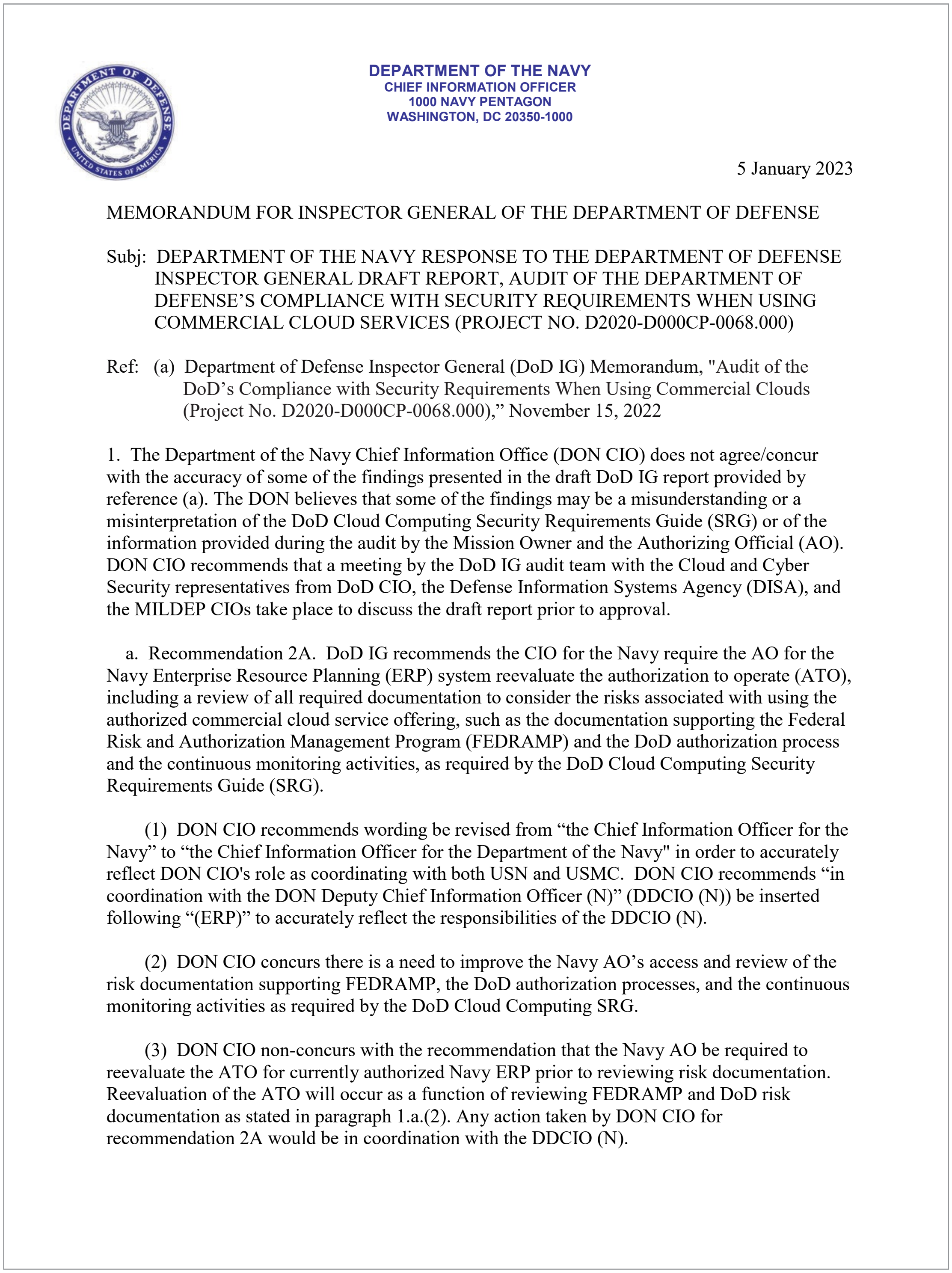
The anticipated completion date for this recommendation will be 30 April 2023.

**Official Army Position**

The Office of the Chief Information Officer (OCIO) concurs with the recommendation and will direct the Authorizing Official (AO) for the DoD Explosives Safety Knowledge Enterprise System to review the Authorization to Operate and all supporting documentation to ensure the system complies with DoD and Army regulations. In particular, AO will ensure that the system complies with the Secure Cloud Computing Architecture and Cloud Computing Security Requirements Guide. The CIO will task the AO in January 2023 with expected completion data by 30 April 2023.

## (U) Department of the Navy Chief Information Officer

Final
Report Reference



DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

5 January 2023

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

Subj: DEPARTMENT OF THE NAVY RESPONSE TO THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL DRAFT REPORT, AUDIT OF THE DEPARTMENT OF DEFENSE'S COMPLIANCE WITH SECURITY REQUIREMENTS WHEN USING COMMERCIAL CLOUD SERVICES (PROJECT NO. D2020-D000CP-0068.000)

Ref: (a) Department of Defense Inspector General (DoD IG) Memorandum, "Audit of the DoD's Compliance with Security Requirements When Using Commercial Clouds (Project No. D2020-D000CP-0068.000)," November 15, 2022

1. The Department of the Navy Chief Information Office (DON CIO) does not agree/concur with the accuracy of some of the findings presented in the draft DoD IG report provided by reference (a). The DON believes that some of the findings may be a misunderstanding or a misinterpretation of the DoD Cloud Computing Security Requirements Guide (SRG) or of the information provided during the audit by the Mission Owner and the Authorizing Official (AO). DON CIO recommends that a meeting by the DoD IG audit team with the Cloud and Cyber Security representatives from DoD CIO, the Defense Information Systems Agency (DISA), and the MILDEP CIOs take place to discuss the draft report prior to approval.

a. Recommendation 2A. DoD IG recommends the CIO for the Navy require the AO for the Navy Enterprise Resource Planning (ERP) system reevaluate the authorization to operate (ATO), including a review of all required documentation to consider the risks associated with using the authorized commercial cloud service offering, such as the documentation supporting the Federal Risk and Authorization Management Program (FEDRAMP) and the DoD authorization process and the continuous monitoring activities, as required by the DoD Cloud Computing Security Requirements Guide (SRG).

(1) DON CIO recommends wording be revised from "the Chief Information Officer for the Navy" to "the Chief Information Officer for the Department of the Navy" in order to accurately reflect DON CIO's role as coordinating with both USN and USMC. DON CIO recommends "in coordination with the DON Deputy Chief Information Officer (N)" (DDCIO (N)) be inserted following "(ERP)" to accurately reflect the responsibilities of the DDCIO (N).

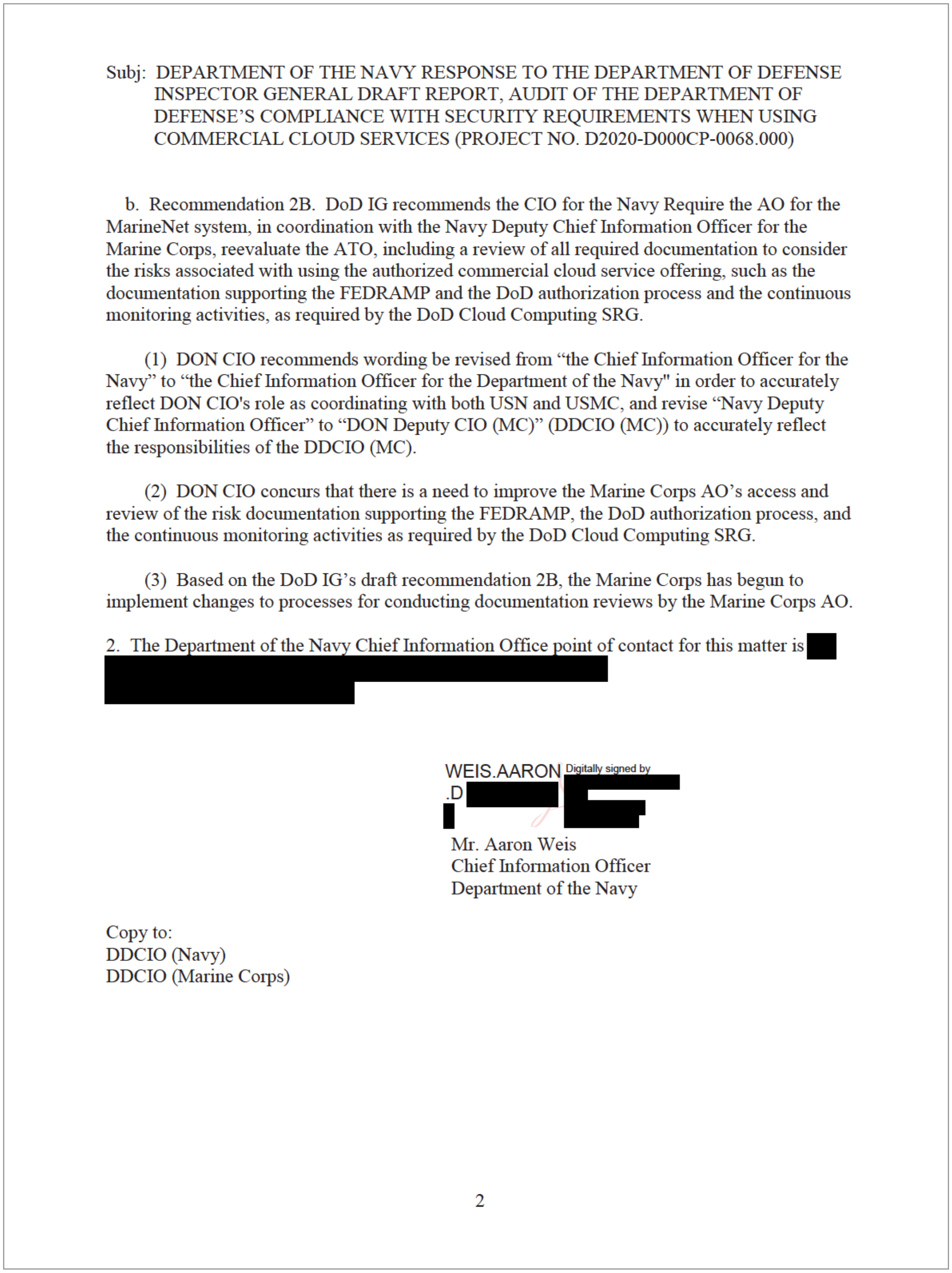
Revised draft
Recommendation 2.a

(2) DON CIO concurs there is a need to improve the Navy AO's access and review of the risk documentation supporting FEDRAMP, the DoD authorization processes, and the continuous monitoring activities as required by the DoD Cloud Computing SRG.

(3) DON CIO non-concurs with the recommendation that the Navy AO be required to reevaluate the ATO for currently authorized Navy ERP prior to reviewing risk documentation. Reevaluation of the ATO will occur as a function of reviewing FEDRAMP and DoD risk documentation as stated in paragraph 1.a.(2). Any action taken by DON CIO for recommendation 2A would be in coordination with the DDCIO (N).

# (U) Department of the Navy Chief Information Officer (cont'd)

**Final Report Reference**



Subj: DEPARTMENT OF THE NAVY RESPONSE TO THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL DRAFT REPORT, AUDIT OF THE DEPARTMENT OF DEFENSE'S COMPLIANCE WITH SECURITY REQUIREMENTS WHEN USING COMMERCIAL CLOUD SERVICES (PROJECT NO. D2020-D000CP-0068.000)

b. Recommendation 2B. DoD IG recommends the CIO for the Navy Require the AO for the MarineNet system, in coordination with the Navy Deputy Chief Information Officer for the Marine Corps, reevaluate the ATO, including a review of all required documentation to consider the risks associated with using the authorized commercial cloud service offering, such as the documentation supporting the FEDRAMP and the DoD authorization process and the continuous monitoring activities, as required by the DoD Cloud Computing SRG.

**Revised draft Recommendation 2.b**

(1) DON CIO recommends wording be revised from "the Chief Information Officer for the Navy" to "the Chief Information Officer for the Department of the Navy" in order to accurately reflect DON CIO's role as coordinating with both USN and USMC, and revise "Navy Deputy Chief Information Officer" to "DON Deputy CIO (MC)" (DDCIO (MC)) to accurately reflect the responsibilities of the DDCIO (MC).

(2) DON CIO concurs that there is a need to improve the Marine Corps AO's access and review of the risk documentation supporting the FEDRAMP, the DoD authorization process, and the continuous monitoring activities as required by the DoD Cloud Computing SRG.

(3) Based on the DoD IG's draft recommendation 2B, the Marine Corps has begun to implement changes to processes for conducting documentation reviews by the Marine Corps AO.

2. The Department of the Navy Chief Information Office point of contact for this matter is [redacted]

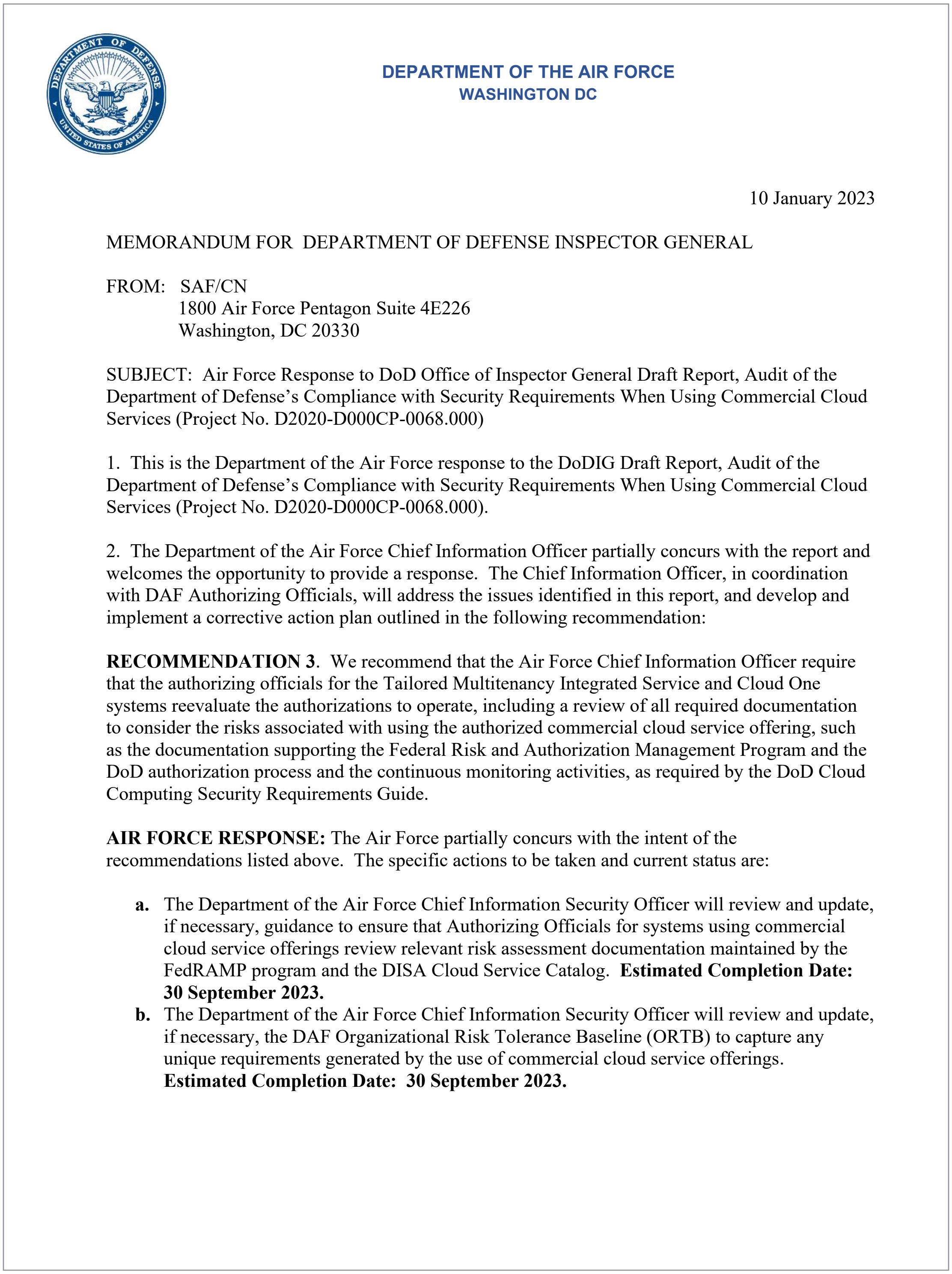
WEIS.AARON.D[redacted] Digitally signed by [redacted]

Mr. Aaron Weis<br>
Chief Information Officer<br>
Department of the Navy

Copy to:<br>
DDCIO (Navy)<br>
DDCIO (Marine Corps)

2

# (U) Department of Air Force



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

10 January 2023

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: SAF/CN
1800 Air Force Pentagon Suite 4E226
Washington, DC 20330

SUBJECT: Air Force Response to DoD Office of Inspector General Draft Report, Audit of the Department of Defense's Compliance with Security Requirements When Using Commercial Cloud Services (Project No. D2020-D000CP-0068.000)

1. This is the Department of the Air Force response to the DoDIG Draft Report, Audit of the Department of Defense's Compliance with Security Requirements When Using Commercial Cloud Services (Project No. D2020-D000CP-0068.000).

2. The Department of the Air Force Chief Information Officer partially concurs with the report and welcomes the opportunity to provide a response. The Chief Information Officer, in coordination with DAF Authorizing Officials, will address the issues identified in this report, and develop and implement a corrective action plan outlined in the following recommendation:

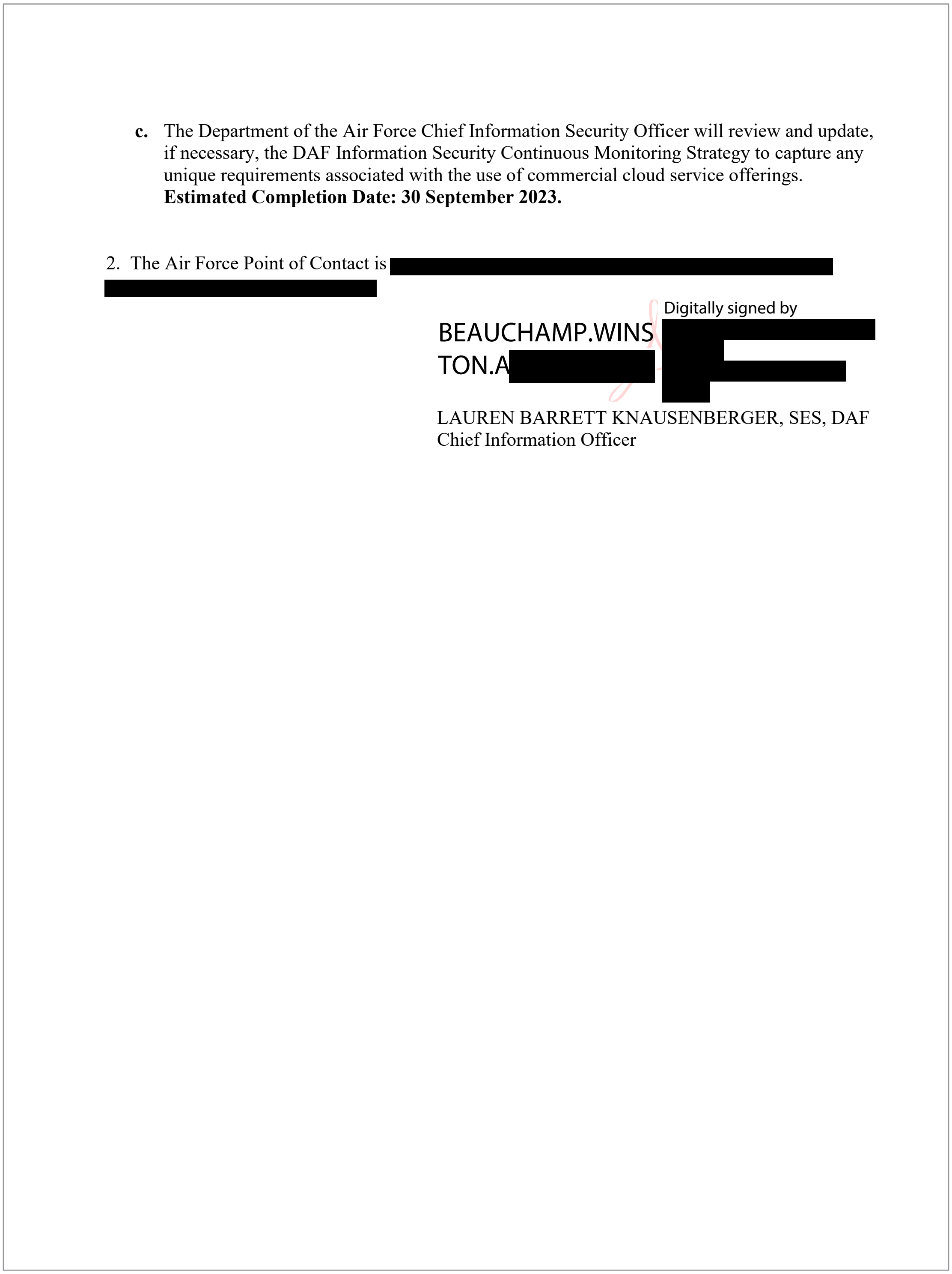
**RECOMMENDATION 3**. We recommend that the Air Force Chief Information Officer require that the authorizing officials for the Tailored Multitenancy Integrated Service and Cloud One systems reevaluate the authorizations to operate, including a review of all required documentation to consider the risks associated with using the authorized commercial cloud service offering, such as the documentation supporting the Federal Risk and Authorization Management Program and the DoD authorization process and the continuous monitoring activities, as required by the DoD Cloud Computing Security Requirements Guide.

**AIR FORCE RESPONSE:** The Air Force partially concurs with the intent of the recommendations listed above. The specific actions to be taken and current status are:

**a.** The Department of the Air Force Chief Information Security Officer will review and update, if necessary, guidance to ensure that Authorizing Officials for systems using commercial cloud service offerings review relevant risk assessment documentation maintained by the FedRAMP program and the DISA Cloud Service Catalog. **Estimated Completion Date: 30 September 2023.**

**b.** The Department of the Air Force Chief Information Security Officer will review and update, if necessary, the DAF Organizational Risk Tolerance Baseline (ORTB) to capture any unique requirements generated by the use of commercial cloud service offerings. **Estimated Completion Date: 30 September 2023.**

## (U) Department of Air Force (cont'd)



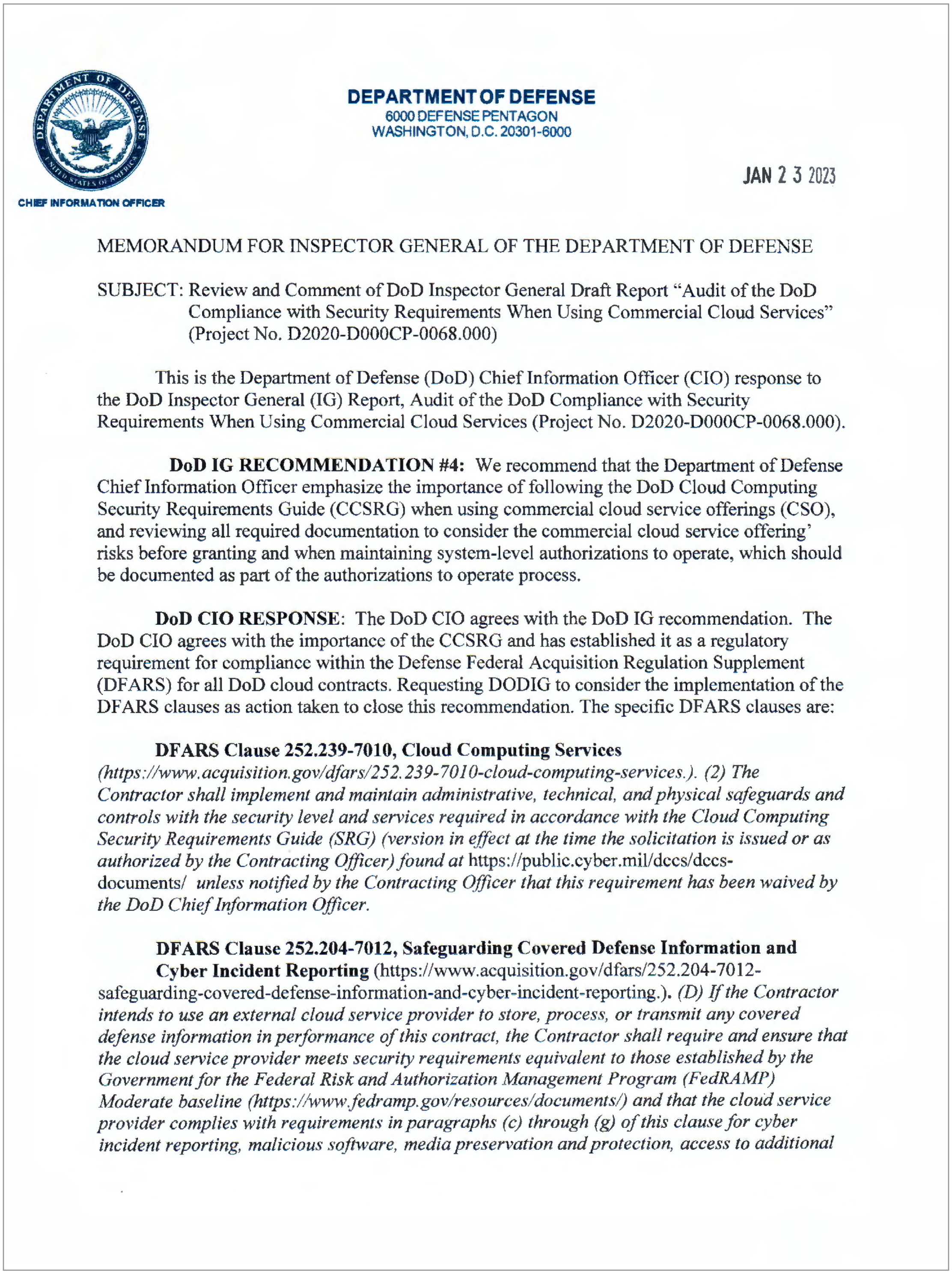
**c.** The Department of the Air Force Chief Information Security Officer will review and update, if necessary, the DAF Information Security Continuous Monitoring Strategy to capture any unique requirements associated with the use of commercial cloud service offerings. **Estimated Completion Date: 30 September 2023.**

2. The Air Force Point of Contact is [redacted]

BEAUCHAMP.WINSTON.A[redacted] Digitally signed by [redacted]

LAUREN BARRETT KNAUSENBERGER, SES, DAF
Chief Information Officer

## (U) The DoD Chief Information Officer



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JAN 2 3 2023

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General Draft Report "Audit of the DoD Compliance with Security Requirements When Using Commercial Cloud Services" (Project No. D2020-D000CP-0068.000)

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General (IG) Report, Audit of the DoD Compliance with Security Requirements When Using Commercial Cloud Services (Project No. D2020-D000CP-0068.000).

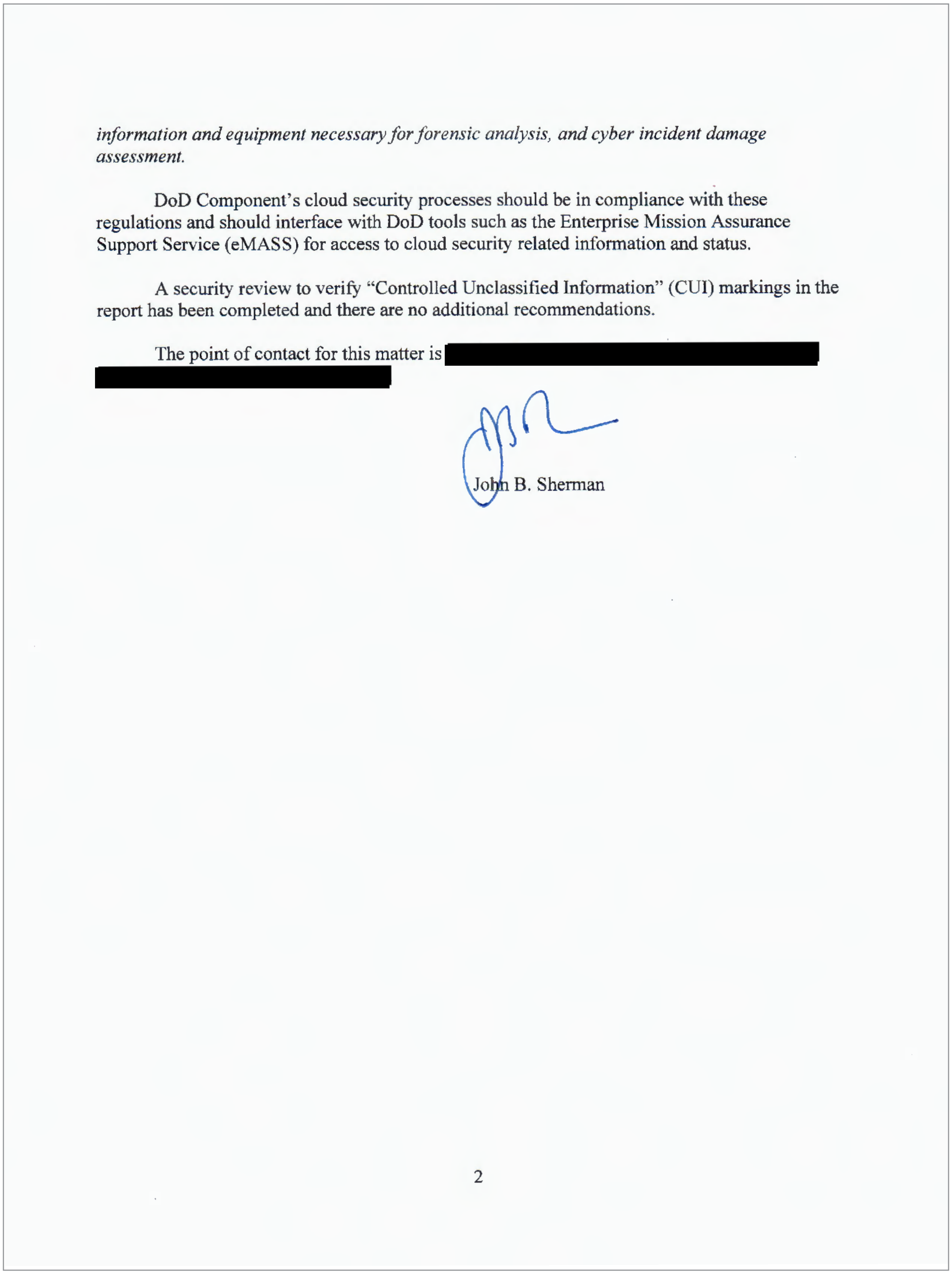
**DoD IG RECOMMENDATION #4:** We recommend that the Department of Defense Chief Information Officer emphasize the importance of following the DoD Cloud Computing Security Requirements Guide (CCSRG) when using commercial cloud service offerings (CSO), and reviewing all required documentation to consider the commercial cloud service offering' risks before granting and when maintaining system-level authorizations to operate, which should be documented as part of the authorizations to operate process.

**DoD CIO RESPONSE**: The DoD CIO agrees with the DoD IG recommendation. The DoD CIO agrees with the importance of the CCSRG and has established it as a regulatory requirement for compliance within the Defense Federal Acquisition Regulation Supplement (DFARS) for all DoD cloud contracts. Requesting DODIG to consider the implementation of the DFARS clauses as action taken to close this recommendation. The specific DFARS clauses are:

**DFARS Clause 252.239-7010, Cloud Computing Services** *(https://www.acquisition.gov/dfars/252.239-7010-cloud-computing-services.). (2) The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time the solicitation is issued or as authorized by the Contracting Officer) found at* https://public.cyber.mil/dccs/dccs-documents/ *unless notified by the Contracting Officer that this requirement has been waived by the DoD Chief Information Officer.*

**DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting** (https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.). *(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional*

# (U) The DoD Chief Information Officer (cont'd)



*information and equipment necessary for forensic analysis, and cyber incident damage assessment.*

DoD Component's cloud security processes should be in compliance with these regulations and should interface with DoD tools such as the Enterprise Mission Assurance Support Service (eMASS) for access to cloud security related information and status.

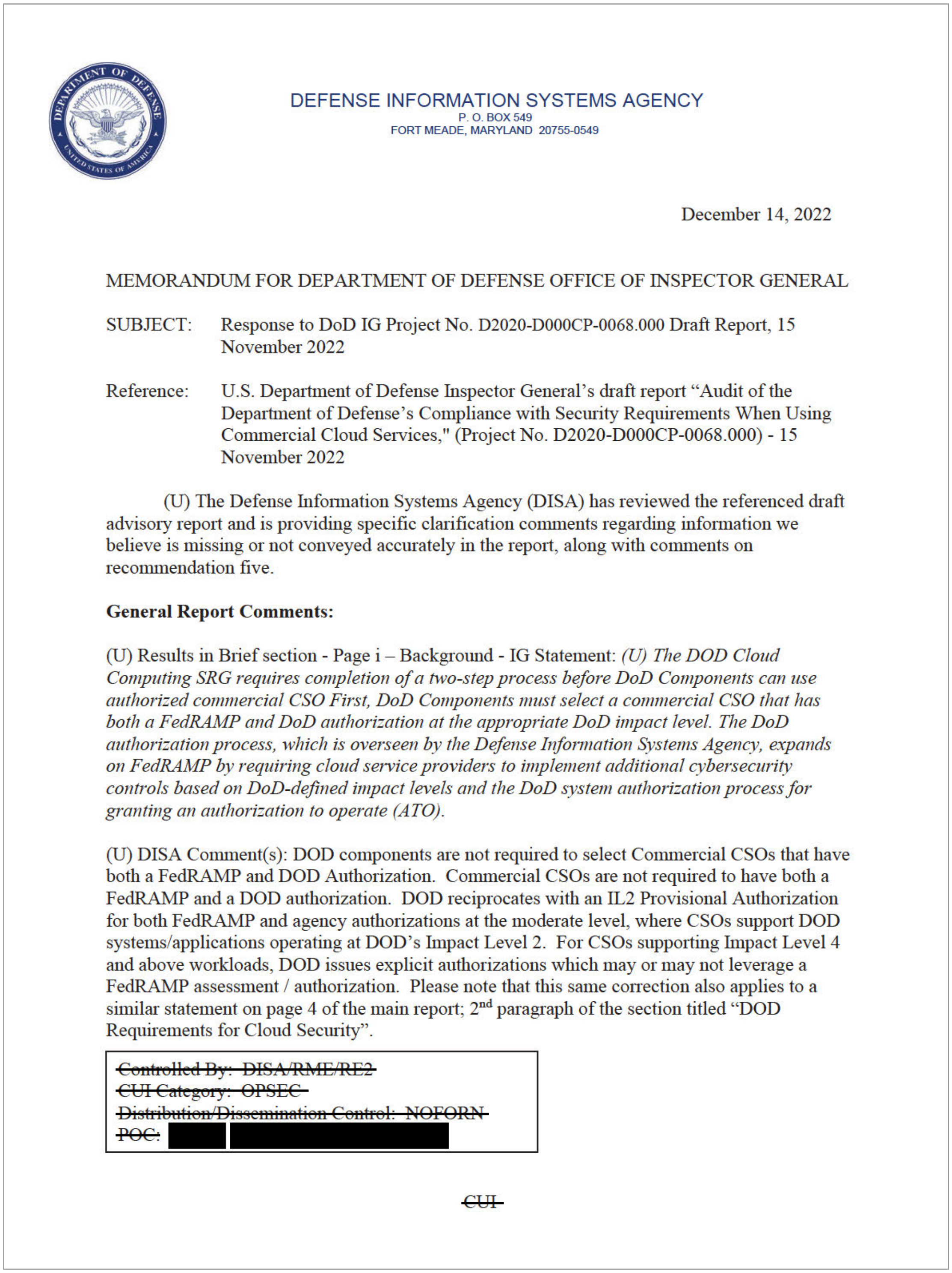
A security review to verify "Controlled Unclassified Information" (CUI) markings in the report has been completed and there are no additional recommendations.

The point of contact for this matter is [redacted]

John B. Sherman

# (U) Defense Information Systems Agency

**Final Report Reference**



DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

December 14, 2022

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

SUBJECT: Response to DoD IG Project No. D2020-D000CP-0068.000 Draft Report, 15 November 2022

Reference: U.S. Department of Defense Inspector General's draft report "Audit of the Department of Defense's Compliance with Security Requirements When Using Commercial Cloud Services," (Project No. D2020-D000CP-0068.000) - 15 November 2022

(U) The Defense Information Systems Agency (DISA) has reviewed the referenced draft advisory report and is providing specific clarification comments regarding information we believe is missing or not conveyed accurately in the report, along with comments on recommendation five.

**General Report Comments:**

(U) Results in Brief section - Page i – Background - IG Statement: *(U) The DOD Cloud Computing SRG requires completion of a two-step process before DoD Components can use authorized commercial CSO First, DoD Components must select a commercial CSO that has both a FedRAMP and DoD authorization at the appropriate DoD impact level. The DoD authorization process, which is overseen by the Defense Information Systems Agency, expands on FedRAMP by requiring cloud service providers to implement additional cybersecurity controls based on DoD-defined impact levels and the DoD system authorization process for granting an authorization to operate (ATO).*

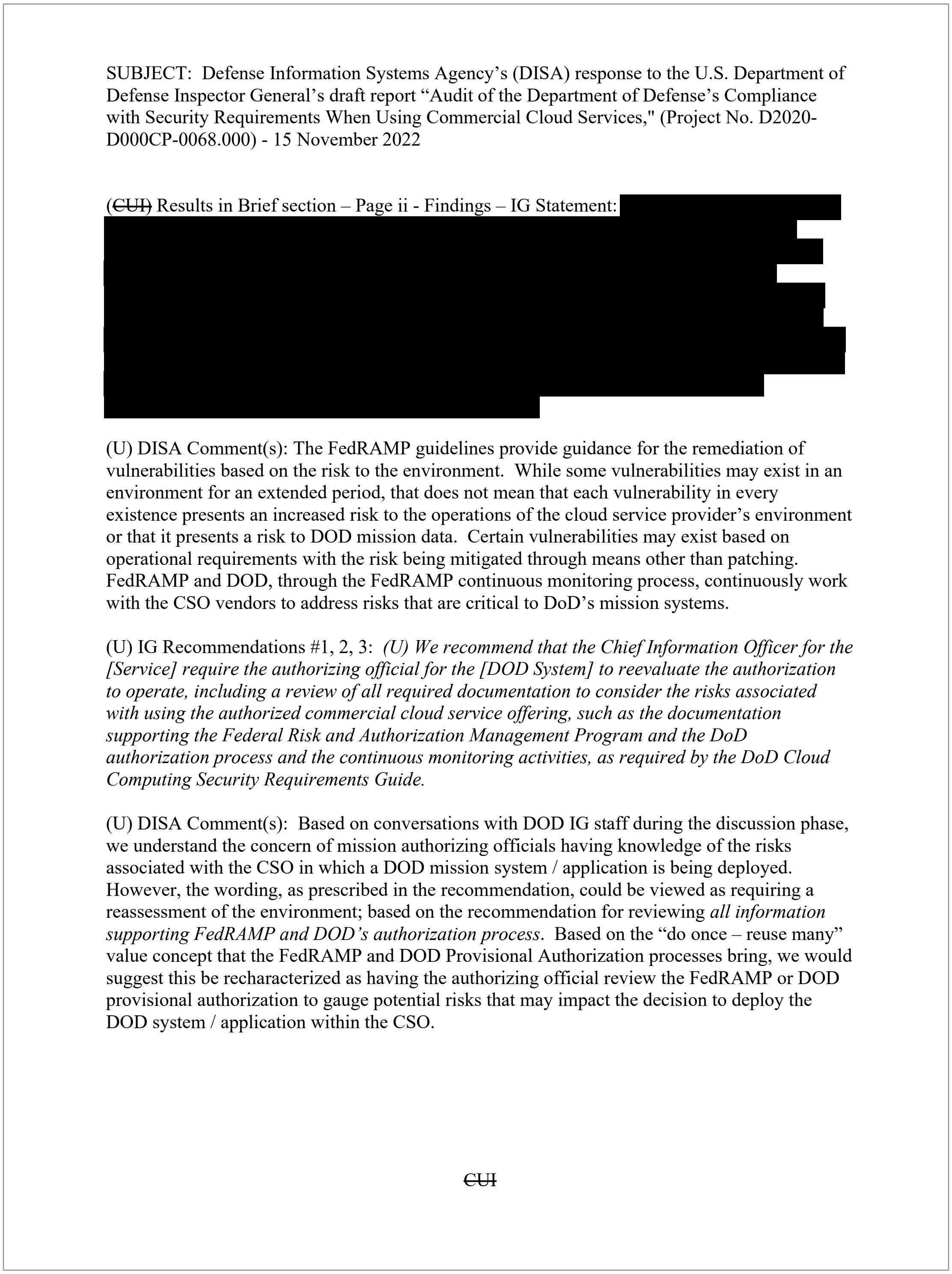
**Revised report pages 5 and 6**

(U) DISA Comment(s): DOD components are not required to select Commercial CSOs that have both a FedRAMP and DOD Authorization. Commercial CSOs are not required to have both a FedRAMP and a DOD authorization. DOD reciprocates with an IL2 Provisional Authorization for both FedRAMP and agency authorizations at the moderate level, where CSOs support DOD systems/applications operating at DOD's Impact Level 2. For CSOs supporting Impact Level 4 and above workloads, DOD issues explicit authorizations which may or may not leverage a FedRAMP assessment / authorization. Please note that this same correction also applies to a similar statement on page 4 of the main report; 2nd paragraph of the section titled "DOD Requirements for Cloud Security".

~~Controlled By: DISA/RME/RE2~~
~~CUI Category: OPSEC~~
~~Distribution/Dissemination Control: NOFORN~~
~~POC:~~ [redacted] [redacted]

~~CUI~~

## (U) Defense Information Systems Agency (cont'd)



SUBJECT: Defense Information Systems Agency's (DISA) response to the U.S. Department of Defense Inspector General's draft report "Audit of the Department of Defense's Compliance with Security Requirements When Using Commercial Cloud Services," (Project No. D2020-D000CP-0068.000) - 15 November 2022

(~~CUI~~) Results in Brief section – Page ii - Findings – IG Statement: [redacted]

(U) DISA Comment(s): The FedRAMP guidelines provide guidance for the remediation of vulnerabilities based on the risk to the environment. While some vulnerabilities may exist in an environment for an extended period, that does not mean that each vulnerability in every existence presents an increased risk to the operations of the cloud service provider's environment or that it presents a risk to DOD mission data. Certain vulnerabilities may exist based on operational requirements with the risk being mitigated through means other than patching. FedRAMP and DOD, through the FedRAMP continuous monitoring process, continuously work with the CSO vendors to address risks that are critical to DoD's mission systems.

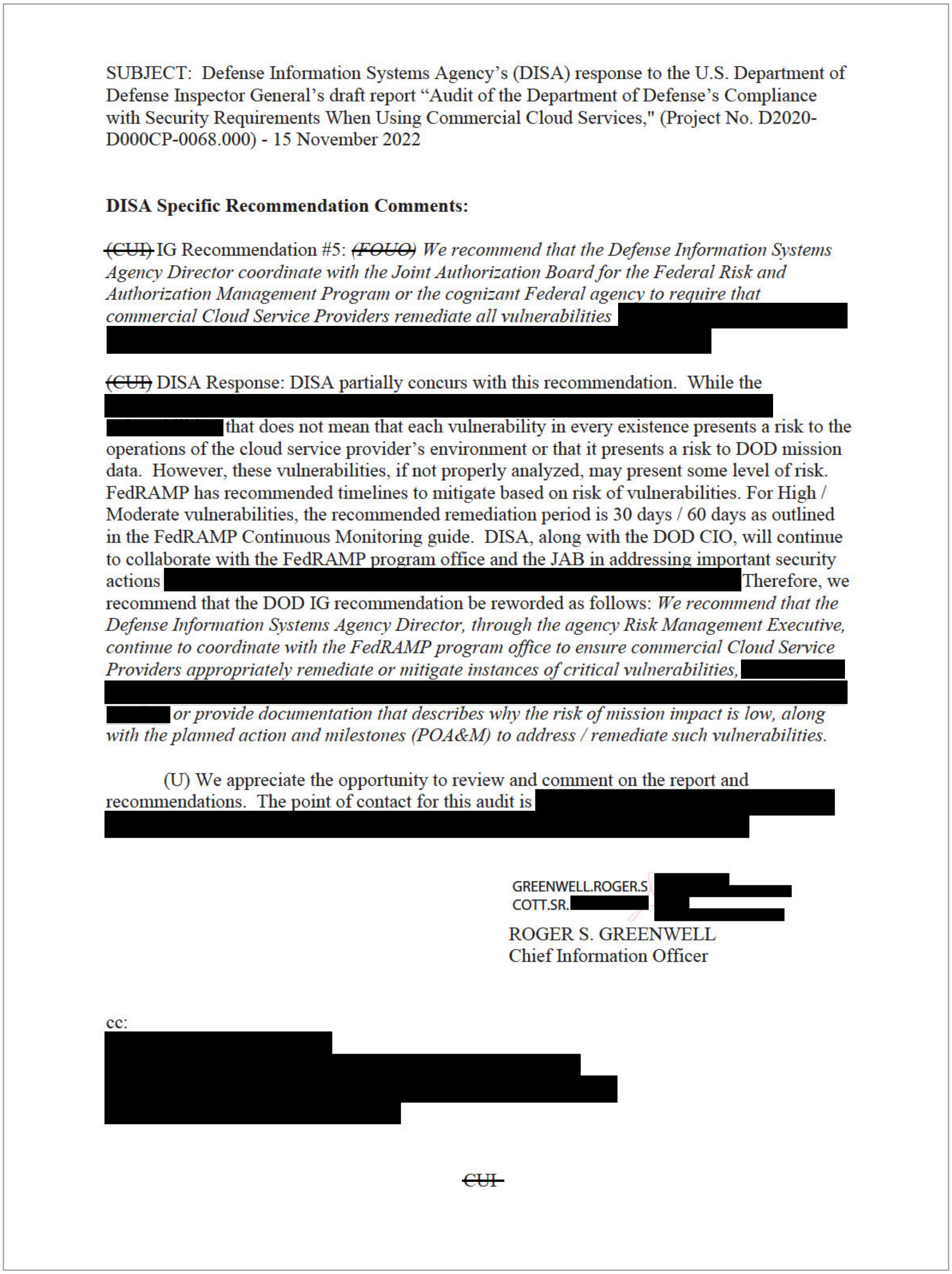
(U) IG Recommendations #1, 2, 3: *(U) We recommend that the Chief Information Officer for the [Service] require the authorizing official for the [DOD System] to reevaluate the authorization to operate, including a review of all required documentation to consider the risks associated with using the authorized commercial cloud service offering, such as the documentation supporting the Federal Risk and Authorization Management Program and the DoD authorization process and the continuous monitoring activities, as required by the DoD Cloud Computing Security Requirements Guide.*

(U) DISA Comment(s): Based on conversations with DOD IG staff during the discussion phase, we understand the concern of mission authorizing officials having knowledge of the risks associated with the CSO in which a DOD mission system / application is being deployed. However, the wording, as prescribed in the recommendation, could be viewed as requiring a reassessment of the environment; based on the recommendation for reviewing *all information supporting FedRAMP and DOD's authorization process*. Based on the "do once – reuse many" value concept that the FedRAMP and DOD Provisional Authorization processes bring, we would suggest this be recharacterized as having the authorizing official review the FedRAMP or DOD provisional authorization to gauge potential risks that may impact the decision to deploy the DOD system / application within the CSO.

~~CUI~~

## (U) Defense Information Systems Agency (cont'd)

**Final**
**Report Reference**



SUBJECT: Defense Information Systems Agency's (DISA) response to the U.S. Department of Defense Inspector General's draft report "Audit of the Department of Defense's Compliance with Security Requirements When Using Commercial Cloud Services," (Project No. D2020-D000CP-0068.000) - 15 November 2022

**DISA Specific Recommendation Comments:**

~~(CUI)~~ IG Recommendation #5: ~~*(FOUO)*~~ *We recommend that the Defense Information Systems Agency Director coordinate with the Joint Authorization Board for the Federal Risk and Authorization Management Program or the cognizant Federal agency to require that commercial Cloud Service Providers remediate all vulnerabilities* [redacted]

~~(CUI)~~ DISA Response: DISA partially concurs with this recommendation. While the [redacted] that does not mean that each vulnerability in every existence presents a risk to the operations of the cloud service provider's environment or that it presents a risk to DOD mission data. However, these vulnerabilities, if not properly analyzed, may present some level of risk. FedRAMP has recommended timelines to mitigate based on risk of vulnerabilities. For High / Moderate vulnerabilities, the recommended remediation period is 30 days / 60 days as outlined in the FedRAMP Continuous Monitoring guide. DISA, along with the DOD CIO, will continue to collaborate with the FedRAMP program office and the JAB in addressing important security actions [redacted] Therefore, we recommend that the DOD IG recommendation be reworded as follows: *We recommend that the Defense Information Systems Agency Director, through the agency Risk Management Executive, continue to coordinate with the FedRAMP program office to ensure commercial Cloud Service Providers appropriately remediate or mitigate instances of critical vulnerabilities,* [redacted] *or provide documentation that describes why the risk of mission impact is low, along with the planned action and milestones (POA&M) to address / remediate such vulnerabilities.*

**Revised draft**
**Recommendation 5**

(U) We appreciate the opportunity to review and comment on the report and recommendations. The point of contact for this audit is [redacted]

GREENWELL.ROGER.S [redacted]
COTT.SR.[redacted]
ROGER S. GREENWELL
Chief Information Officer

cc:
[redacted]

~~CUI~~

# (U) Acronyms and Abbreviations

| | |
|---|---|
| **(U) 3PAO** | Third-party Assessment Organization |
| **(U) AO** | Authorizing Official |
| **(U) ATO** | Authorization to Operate |
| **(U) CIO** | Chief Information Officer |
| **(U) CSO** | Cloud Service Offering |
| **(U) CSP** | Cloud Service Provider |
| **(U) DFARS** | Defense Federal Acquisition Regulation Supplement |
| **(U) DISA** | Defense Information Systems Agency |
| **(U) FedRAMP** | Federal Risk and Authorization Management Program |
| **(U) GAO** | Government Accountability Office |
| **(U) JAB** | Joint Authorization Board |
| **(U) NIST** | National Institute of Standards and Technology |
| **(U) OIG** | Office of Inspector General |
| **(U) OMB** | Office of Management and Budget |
| **(U) POA&M** | Plan of Action and Milestones |
| **(U) RMF** | Risk Management Framework |
| **(U) SRG** | Security Requirements Guide |

# (U) Glossary

**(U) Authorization to Operate (ATO).** A management decision given by a Component's AO to authorize operation of an information system on behalf of the Component that accepts the risks of using the system.

**(U) Authorizing Official (AO).** An official with the authority to formally assume responsibility for the operation of an information system at an acceptable level of risk to agency operations.

**(U) Cloud Environment.** The product of a CSO for virtual use and storage of information which is categorized into three categories: Infrastructure as a Service, Platform as a Service, and Software as a Service.

**(U) Cloud Services.** A wide range of services delivered on demand by CSPs to companies and customers over the Internet.

**(U) Cloud Service Offering (CSO).** Cloud services offered by CSPs that are commercially available for purchase. For the DoD, the CSO is required to be assessed by the FedRAMP and DoD risk management framework processes and is approved for Components' use.

**(U) Cloud Service Provider (CSP).** A company that provides cloud services for purchase.

**(U) DoD Authorization.** The authorization process the DISA performs on cloud services to ensure that the CSO meets DoD cloud security standards.

**(U) Federal Risk and Authorization Management Program (FedRAMP) Authorization.** A cost-effective, risk-based approach for the adoption and use of cloud services by the Government.

**(U) Impact Level.** The sensitivity or confidentiality level of information that is stored and processed in a CSP environment. The DoD has four impact levels: 2, 4, 5, and 6.

**(U) Risk Management Framework (RMF).** The structured process used to identify potential threats and define a strategy for eliminating or minimizing the associated risks.

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

## 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/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at 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; 703.604.8324

**DoD OIG Mailing Lists**
www.dodig.mil/Mailing-Lists/

**Twitter**
www.twitter.com/DoD_IG

**DoD Hotline**
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098