OIG
Office of Inspector General
U.S. Department of State • Broadcasting Board of Governors

AUD-IT-17-56 Office of Audits August 2017

Management Assistance Report: The Process to Authorize and Track Information Technology Systems Needs Improvement

INFORMATION TECHNOLOGY DIVISION

Summary of Review

Security safeguards must be in place to protect automated information systems and data from unauthorized access, modifications, and destruction. One such safeguard is periodically assessing the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls. At the Department of State (Department), this practice is known as the System Authorization Process and results in a formal declaration by the Designated Approving Authority authorizing the operation of a system. An Authorization to Operate (ATO) is signed by the Designated Approving Authority after a security controls assessor[1] certifies that the system has met and passed all requirements to become operational. Within the Department, the Chief Information Officer (CIO) is the Designated Approving Authority[2] that authorizes the operation of a system and determines the system's expiration date.

According to Department guidance, the Bureau of Information Resource Management (IRM), Information Assurance Division must ensure system authorizations are performed for Department information systems in accordance with the Department's System Authorization Process Guide.[3] However, the Office of Inspector General (OIG) has identified instances where system authorizations have not been performed. Specifically, OIG found that four of five systems assessed during a compliance follow-up audit of the Department's access controls for major applications[4] did not have a current ATO.

In addition, OIG was unable to determine an accurate source for tracking Federal Information Security Management Act (FISMA) reportable systems and other Department assets that require an ATO. Specifically, OIG identified ATO tracking mechanisms that reported inconsistent inventory of FISMA reportable systems. For example, the Department's official inventory for information technology assets, iMatrix,[5] reports 396 FISMA reportable assets. IRM's Information Assurance Division is separately tracking 413 FISMA reportable system through an Excel spreadsheet. Finally, the "CIO Quarter Two FISMA Report" identified 549 FISMA reportable assets.

[1] The security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls and control enhancements employed within or inherited by an information system to determine the overall effectiveness of the controls. (National Institute of Standards and Technology, Special Publication 800-37, rev 1).

[2] The CIO is the Designated Approving Authority for unclassified and classified systems, including collateral Top Secret. (Foreign Affairs Handbook (FAH), 5 FAH-11 H-412.1, "Designated Approval Authority (DAA)," and the Foreign Affairs Manual (FAM), 1 FAM 271.1, "Policy").

[3] 5 FAM 1066.1-3 (A), "Department Information Systems."

[4] As of June 2017, OIG's compliance follow-up audit of the Department's access controls for major applications is ongoing.

[5] iMatrix is the Department's information technology portfolio management tool that serves as the single authoritative source for information on Department technology investments, programs, projects, and assets. System or business owners must register their data assets in iMatrix and update the entries on a regular basis. (5 FAH-8 H-116, "Definitions," and 5 FAM 639.1, "Enterprise Data Inventory").

According to iMatrix, 54 percent[6] of FISMA reportable systems[7] have expired ATOs, and 23 percent[8] of the FISMA reportable systems did not identify the ATO expiration dates. Therefore, collectively, 77 percent (303 of 396 systems) of all FISMA reportable assets may be noncompliant with the Department's System Authorization Process and standards prescribed by the National Institute of Standards and Technology (NIST). Without ensuring that the System Authorization Process is performed on its information technology systems and that iMatrix or another designated repository contains complete and accurate information (including the expiration dates of ATOs), the Department's ability to protect these systems and safeguard the confidentiality, integrity, and availability of the system and its information is significantly hampered.

OIG is recommending the following:

- IRM formally designate a central repository to track the status of systems authorizations and documentation for Department information systems, including Federal Information Security Management Act reportable systems.

- The Bureau of Consular Affairs (CA), in coordination with IRM, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for Consular Consolidated Database (CCD) and Passport Information Electronic Records System (PIERS).

- The Bureau of Diplomatic Security (DS), also in coordination with IRM, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Classified Investigative Management System (IMS-C) and SY Namecheck (SYNCH).

- IRM develop and implement a corrective action plan to ensure it fully complies with Department policy relating to the System Authorization Process for all applicable information technology systems.

On the basis of the Department's response to a draft of this report, OIG considers two recommendations closed and five recommendations resolved, pending further action. A synopsis of the Department's response to the recommendations and OIG's reply follow each recommendation. Responses from Management to a draft of this report are reprinted in their entirety in Appendices B, C, and D.

[6] Based on the iMatrix asset inventory provided by IRM, the total population is 4,289 assets, and 396 of those assets are FISMA reportable systems. Of the FISMA reportable systems, 212 are categorized with expired ATO dates.

[7] FISMA reportable inventory consists of major information systems set forth in Federal Information Processing Standard (FIPS) Publication 199 and includes agency systems, contractor systems, and websites.

[8] As noted previously, the iMatrix asset inventory identifies 396 assets as FISMA reportable systems. Of those FISMA reportable systems, 91 did not have an ATO date listed.

BACKGROUND

FISMA[9] requires major information systems[10] to be inventoried, assessed and authorized, and reported to the Office of Management and Budget. FISMA's objective is to provide a comprehensive framework for ensuring the effectiveness of information security controls[11] over information resources that support Federal operations and assets. FISMA assigned NIST to develop standards, guidelines and associated methods and techniques for information systems.

NIST,[12] in partnership with other Federal agencies,[13] has developed a Risk Management Framework for use by the Federal Government and its contractors, for the purpose of improving information security, strengthening risk management processes, and encouraging reciprocity among Federal agencies.[14] According to NIST Special Publication 800-37 rev. 1, there are six steps within the Risk Management Framework, one of which is to authorize the information system (see Appendix A).

The Department's System Authorization Process implements the NIST Risk Management Framework.[15] Department policy[16] requires that security authorizations be performed on all Department information systems, as well as non-Department systems that process information on behalf of the Department. This process involves (1) comprehensively testing and evaluating security features (also known as controls) to determine the risk to organizational operations and assets, individuals, other organizations, and the nation for operating the information system, and (2) deciding that this risk is acceptable. It addresses software and hardware security

[9] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled FISMA, emphasizes that organizations should develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets. (NIST SP 800-37, rev. 1).

[10] Major information systems are those systems that require special management attention because of their importance to an agency mission; their high development, operating, or maintenance costs; or their significant role in the administration of agency programs, finances, property, or other resources with a FIPS 199 Impact level of high or moderate (NIST 800-18, rev. 1). According to NIST SP 800-37, rev. 1, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[11] Security controls are the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (NIST SP 800-37, rev. 1).

[12] NIST is a Federal agency under the Department of Commerce. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems.

[13] Partners include the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems (NIST SP 800-37, rev. 1).

[14] NIST SP 800-37 rev. 1), *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach* (June 2014).

[15] This analysis is based on the information provided in the Department's System Authorization Guide on the IRM/ Information Assurance Division website, "Assessment and Authorization Toolkit," http://irm.m.state.sbu/sites/ia.SiteDirectory/ca/Pages/default.aspx, accessed March 8, 2017.

[16] 5 FAM 1066.1-3 (A), "Department Information Systems"; 5 FAH-11 H-411.3, "Scope"; 5 FAH-11 H-412.4, "Sponsoring Bureau."

safeguards; considers procedural, physical, and personnel security measures; and establishes the extent to which a particular design (or architecture), configuration, and implementation meets a specified set of security requirements throughout the life cycle of the information system. It also considers procedural, physical, and personnel security measures employed to enforce information security policy.[17]

Purpose of this Management Assistance Report and Ongoing Compliance Follow-up Audit

This Management Assistance Report is intended to provide early communication of deficiencies that OIG identified during its ongoing compliance follow-up audit of the Department's access controls for major applications. The primary objective of the compliance follow-up audit is to determine whether the Department's actions to address selected recommendations from the *Audit of the Department of State's Access Controls for Major Applications*[18] corrected the deficiencies identified in that 2012 report regarding logical access controls.

In performing the work related to these deficiencies, OIG interviewed the Information System Security Officer for IMS-C, SYNCH, CCD, PIERS and Classified State Messaging and Archive Retrieval Toolset. Below is a brief description of each system:

- IMS-C captures all classified investigative case related information; automates, integrates and improves the investigative business processes; establishes a central index encompassing all Diplomatic Security Service classified investigations; and provides investigative/intelligence analysis and analytical processing while creating internal and external electronic data sharing.

- SYNCH automates the tasks associated with tracking personnel clearance status and clearance folder locations. The application maintains information on clearance type and status, case open and close dates, clearance dates, investigation type, case code and number, and folder location.

- CCD is a central data storehouse of current and archived data from CA's post databases around the world as well as domestic applications. It allows users access to multiple reports, forms, and authenticated links to other systems and across applications. Some of the integrated data in CCD is the Master Death File[19] from the Social Security Administration and name check responses from the Government of Canada's Citizenship and Immigration Agency.

[17] Department of Homeland Security, *Security Authorization Guide*, March 16, 2015, https://www.dhs.gov/sites/default/files/publications/Security%20Authorization%20Process%20Guide_v11_1.pdf.

[18] OIG, *Audit of Department of State Access Controls for Major Applications* (AUD-IT-12-44, September 2012).

[19] The Master Death File contains over 83 million records of deaths that have been reported to the Social Security Administration. This file includes the person's social security number, name, date of birth, and date of death.

- PIERS is the single web portal for all passport data. This data includes information such as records of issued and expired passports; applications that are not issued; destroyed, stolen, or lost passports; and Consular records of overseas births and deaths.

RESULTS

An ATO is the official management decision given by the Department's Designated Approving Authority to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation. This decision is based on the implementation of an agreed-upon set of security controls. An information system must be granted an ATO through an official accreditation decision memorandum from the Designated Approving Authority, before becoming operational and must be reauthorized at least every 3 years[20] or whenever changes are made that affect the potential risk level of operating the system. The reauthorization process typically begins 4 to 6 months before the ATO is set to expire. The Designated Approving Authority reviews the Security Authorization Package, determines the degree of acceptable risk based on mission requirements, accepts security responsibility for the operation of an assessed system, and officially grants or denies the system an ATO.

OIG found that four of five systems assessed during its compliance follow-up audit of the Department's access controls for major applications did not have a current ATO. Specifically, OIG found the ATOs for two systems expired in 2016 and the ATOs for another two systems expired on March 31, 2017. Table 1 lists the FISMA reportable systems assessed during OIG's compliance follow-up audit that did not have current ATOs and the expiration date of the ATO recorded in iMatrix.

Table 1: FISMA Reportable Systems and Associated Expiration Date of the ATO, as of May 2017

System	ATO Expiration Date
Investigative Management System (IMS-C)	March 31, 2017
SY Namecheck (SYNCH)	October 31, 2016
Consular Consolidated Database (CCD)	March 31, 2016
Passport Information Electronic Records System (PIERS)	March 31, 2017

Source: Generated by OIG based on the authorization memoranda for IMS-C, SYNCH, CCD and PIERS.

According to Department policy, iMatrix is the Department's official inventory for IT assets, and registration in iMatrix is required for portfolio management purposes. However, OIG did not

[20] This analysis is based on the information provided in the Department's System Authorization Guide on the IRM/ Information Assurance Division website, "Assessment and Authorization Toolkit," http://irm.m.state.sbu/sites/ia.SiteDirectory/ca/Pages/When_Required.aspx, accessed March 8, 2017.

identify a specific policy requiring documentation of the information Systems Authorization Process in iMatrix. When OIG inquired about the method used by the Department to track system authorization for information assets, an IRM official stated that the Information Assurance Division tracks the ATO status via a database that consists of an Excel spreadsheet. Upon analysis of that Excel spreadsheet, OIG determined the Information Assurance Division is tracking 783 IT assets, while iMatrix is tracking 4,289 IT assets. Therefore, Information Assurance Division is tracking 783 of 4,289 (18 percent) of the IT assets registered in iMatrix.

In addition, the number of reportable FISMA systems being tracked in the Department is not consistent. For example, iMatrix reports 396 FISMA reportable assets, IRM's Information Assurance Division reports 413 FISMA reportable assets, and the "Chief Information Officer 2017 Quarter 2 FISMA Report" identified 549 FISMA reportable assets. An IRM official stated that the metrics for the CIO's quarterly report are derived from the Information Assurance Division's database. IRM also stated that the inventory database is not static and that, the inventory could therefore vary at different points in time. However, OIG noted that the CIO's quarterly report included 136 IT assets that were not accounted for in the Information Assurance Division's database.

The Department is also not consistently ensuring compliance with standards relating to ATOs. According to iMatrix, there are 396 FISMA reportable assets. Of the 396 systems, 212 (54 percent) of the FISMA reportable systems have expired ATOs, and 91 of 396 (23 percent) of the FISMA reportable systems did not have ATO expiration dates identified in iMatrix. Therefore, collectively, 303 of 396 (77 percent) of all FISMA reportable assets are noncompliant with the Department's System Authorization Process and the standards prescribed by NIST.

CONCLUSION

Both Department guidance and standards prescribed by NIST underscore the importance of periodically assessing the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls. However, OIG found that 77 percent of the Department's FISMA reportable IT assets are noncompliant, based on information contained in iMatrix, as of May 2017. The System Authorization Process needs to be performed and documented for the Department's IT systems and iMatrix (or another designated repository) to ensure that it contains complete and accurate information, including the expiration dates of ATOs. Without this, the Department's ability to protect these systems and safeguard the confidentiality, integrity, and availability of the system and its information is significantly hampered.

> **Recommendation 1:** OIG recommends that the Bureau of Information Resource Management formally designate a central repository to track the status of systems authorizations and documentation for Department information systems, including Federal Information Security Management Act reportable systems.

Management Response: IRM concurred with this recommendation, stating that it has "procured and developed a governance, risk, and compliance system called Xacta to act as the central repository to track the status of systems authorizations and documentation for Department information systems," including FISMA reportable systems. According to IRM, the system is scheduled "to go into production before the end of August 2017."

OIG Reply: On the basis of IRM's concurrence with this recommendation and its planned actions, OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has formally designated a central repository to track the status of systems authorizations and documentation for Department information systems.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management update Department policies and procedures to reflect the designation of the central repository in Recommendation 1.

Management Response: IRM concurred with this recommendation, stating it "will codify the necessary changes to applicable policy and procedures and work to incorporate these changes into current guidance." IRM plans to provide interim guidance to the Department until current guidance is updated.

OIG Reply: On the basis of IRM's concurrence with this recommendation and its planned actions, OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has updated Department policies and procedures to reflect the designation of the central repository in Recommendation 1.

Recommendation 3: OIG recommends that the Bureau of Consular Affairs, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Consular Consolidated Database.

Management Response: CA concurred with this recommendation stating that the Systems Authorization Process was completed for CCD in July 2017 and has an ATO in place.

OIG Reply: OIG considers this recommendation closed. OIG reviewed the authorization memorandum for CCD provided by CA and confirmed that CA had completed the System Authorization Process in July 2017.

Recommendation 4: OIG recommends that the Bureau of Consular Affairs, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Passport Information Electronic Records System.

Management Response: CA stated that PIERS is listed as a subcomponent in the Passport Application Management System ATO. This ATO had expired, but CA subsequently obtained an extension to the ATO in May 2017. The extended ATO expires on July 31, 2019.

OIG Reply: OIG considers this recommendation closed. OIG reviewed the documentation provided by CA and confirmed that CA had obtained an extension to the ATO in May 2017.

Recommendation 5: OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Classified Investigative Management System.

Management Response: DS concurred with this recommendation.

OIG Reply: On the basis of DS's concurrence with this recommendation, OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that DS completed the Systems Authorization Process with an authorization memorandum for the IMS-C.

Recommendation 6: OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the SY Namecheck.

Management Response: DS concurred with this recommendation.

OIG Reply: On the basis of DS's concurrence with this recommendation, OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that DS completed the Systems Authorization Process with an authorization memorandum for SYNCH.

Recommendation 7: OIG recommends that the Bureau of Information Resource Management develop and implement a corrective action plan that addresses how the Department will comply with Department policy on the Systems Authorization Process. The corrective action plan should identify the root cause of compliance failures, action steps to resolve such compliance failures, improvement benchmarks and a timeframe for completion, and an escalation process to hold system owners accountable.

Management Response: IRM concurred with this recommendation, stated that it will develop the necessary corrective action plans, incorporating all of the OIG's recommendation in said plan.

OIG Reply: On the basis of IRM's concurrence with this recommendation and its planned actions, OIG considers this recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has developed and implemented a corrective action plan that addresses how the Department will comply with the policy on the Systems Authorization Process.

RECOMMENDATIONS

Recommendation 1: OIG recommends that the Bureau of Information Resource Management formally designate a central repository to track the status of systems authorizations and documentation for Department information systems, including Federal Information Security Management Act reportable systems.

Recommendation 2: OIG recommends that the Bureau of Information Resource Management update Department policies and procedures to reflect the designation of the central repository in Recommendation 1.

Recommendation 3: OIG recommends that the Bureau of Consular Affairs, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Consular Consolidated Database.

Recommendation 4: OIG recommends that the Bureau of Consular Affairs, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Passport Information Electronic Records System.

Recommendation 5: OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Classified Investigative Management System.

Recommendation 6: OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the SY Namecheck.

Recommendation 7: OIG recommends that the Bureau of Information Resource Management develop and implement a corrective action plan that addresses how the Department will comply with Department policy on the Systems Authorization Process. The corrective action plan should identify the root cause of compliance failures, action steps to resolve such compliance failures, improvement benchmarks and a timeframe for completion, and an escalation process to hold system owners accountable.

APPENDIX A: RISK MANAGEMENT FRAMEWORK STEPS

According to National Institute of Standards and Technology (NIST), Special Publication 800-37 rev. 1, there are six steps within the risk management framework:

- Step 1: Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- Step 2: Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
- Step 3: Implement the security controls and describe how the controls are employed within the information system and its environment of operation.
- Step 4: Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Step 5: Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- Step 6: Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.[1]

During the authorization phase, steps one through four are completed and a security authorization package is prepared for the Designated Approving Authority's approval. The security authorization package contains: (1) the security plan;[2] (2) the security assessment report;[3] and (3) the plan of action and milestones.[4] The information in these key documents is used by the Designated Approving Authority to make a risk-based authorization decision to either grant or deny the system the Authorization to Operate through an official accreditation decision memorandum.

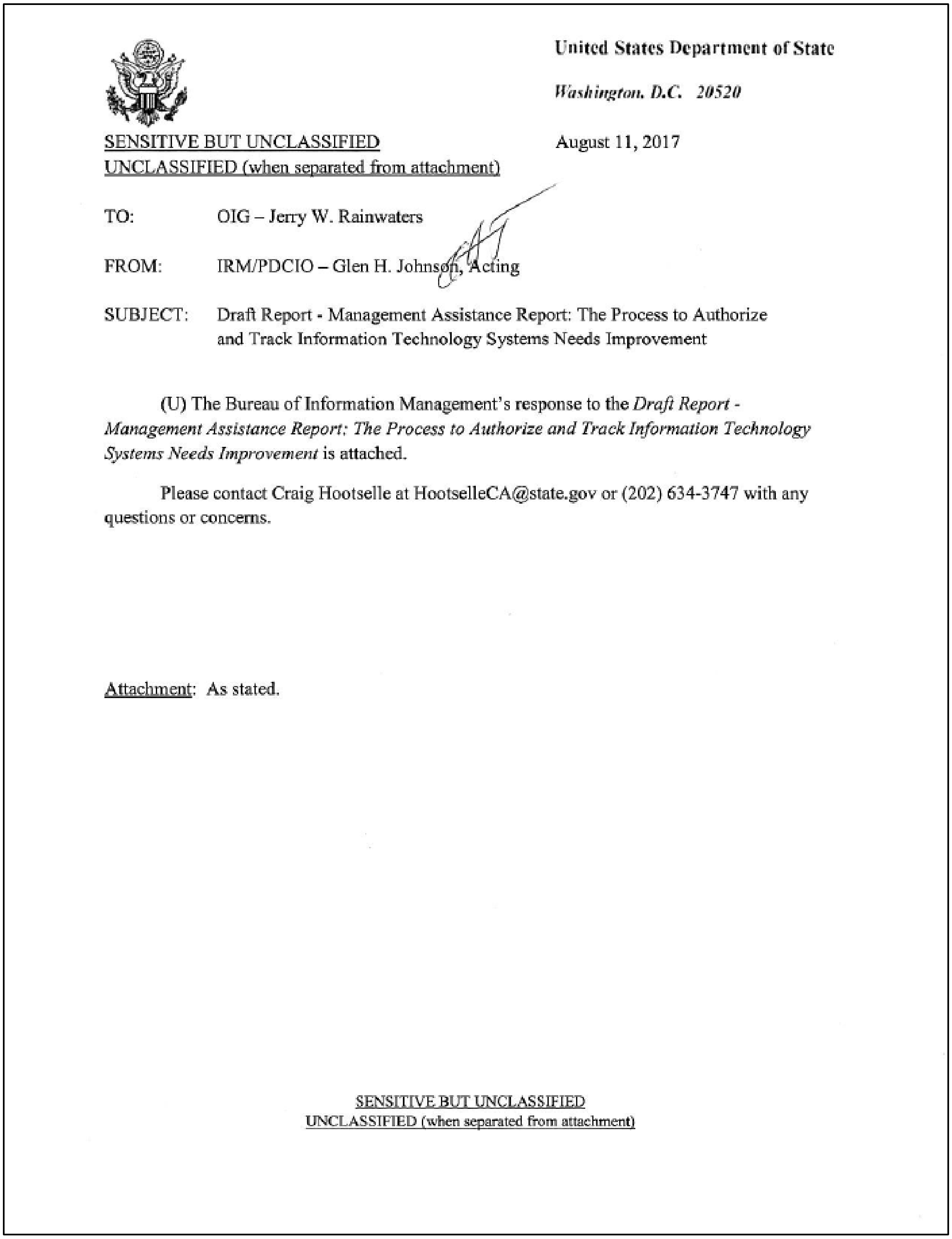
[1] NIST Special Publication 800-37 rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach* (June 2014).

[2] A security plan is a formal document that provides an overview of the security requirements for an information system or an information security program and describes the planned or established security controls for meeting those requirements (NIST SP 800-37, rev. 1).

[3] The security assessment report contains the results and findings from the assessment that was prepared by the security control assessors (NIST SP 800-37, rev. 1).

[4] The plan of action and milestones is a document that identifies tasks that should be performed. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones (NIST SP 800-37, rev. 1).

APPENDIX B: BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE



United States Department of State

Washington, D.C. 20520

SENSITIVE BUT UNCLASSIFIED
UNCLASSIFIED (when separated from attachment)

August 11, 2017

TO: OIG – Jerry W. Rainwaters

FROM: IRM/PDCIO – Glen H. Johnson, Acting

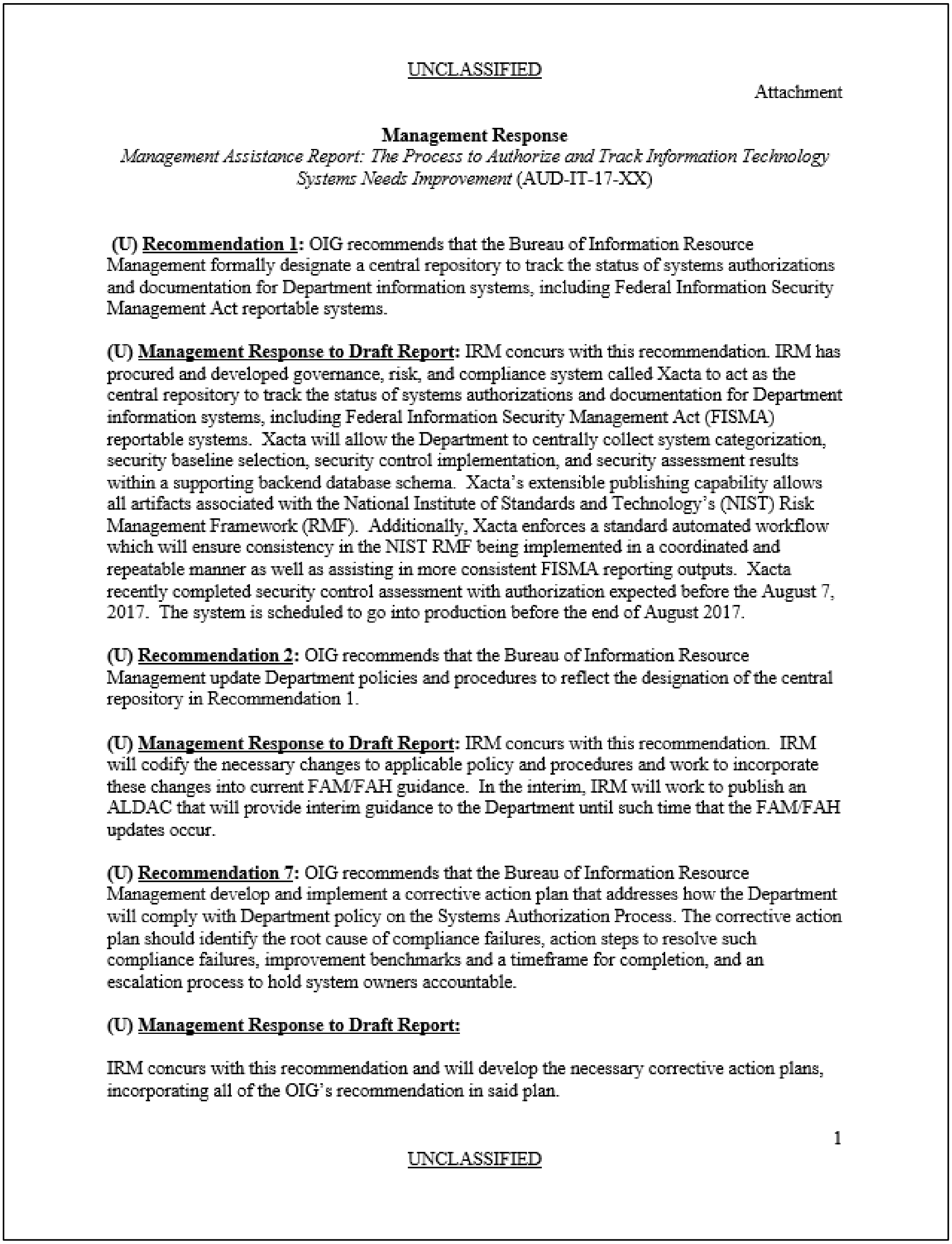
SUBJECT: Draft Report - Management Assistance Report: The Process to Authorize and Track Information Technology Systems Needs Improvement

(U) The Bureau of Information Management's response to the *Draft Report - Management Assistance Report: The Process to Authorize and Track Information Technology Systems Needs Improvement* is attached.

Please contact Craig Hootselle at HootselleCA@state.gov or (202) 634-3747 with any questions or concerns.

Attachment: As stated.

SENSITIVE BUT UNCLASSIFIED
UNCLASSIFIED (when separated from attachment)



Attachment

Management Response

Management Assistance Report: The Process to Authorize and Track Information Technology Systems Needs Improvement (AUD-IT-17-XX)

(U) Recommendation 1: OIG recommends that the Bureau of Information Resource Management formally designate a central repository to track the status of systems authorizations and documentation for Department information systems, including Federal Information Security Management Act reportable systems.

(U) Management Response to Draft Report: IRM concurs with this recommendation. IRM has procured and developed governance, risk, and compliance system called Xacta to act as the central repository to track the status of systems authorizations and documentation for Department information systems, including Federal Information Security Management Act (FISMA) reportable systems. Xacta will allow the Department to centrally collect system categorization, security baseline selection, security control implementation, and security assessment results within a supporting backend database schema. Xacta's extensible publishing capability allows all artifacts associated with the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF). Additionally, Xacta enforces a standard automated workflow which will ensure consistency in the NIST RMF being implemented in a coordinated and repeatable manner as well as assisting in more consistent FISMA reporting outputs. Xacta recently completed security control assessment with authorization expected before the August 7, 2017. The system is scheduled to go into production before the end of August 2017.

(U) Recommendation 2: OIG recommends that the Bureau of Information Resource Management update Department policies and procedures to reflect the designation of the central repository in Recommendation 1.

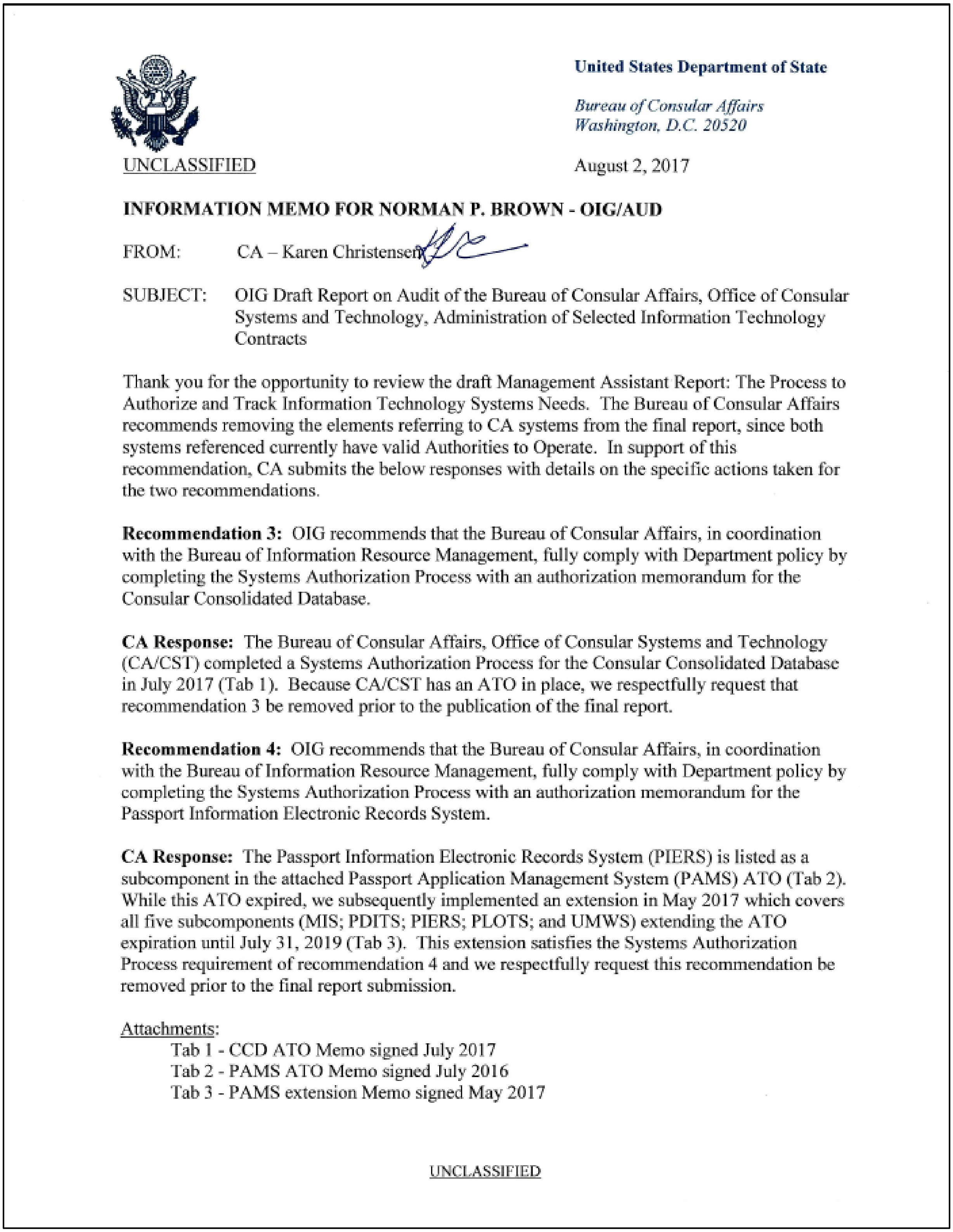
(U) Management Response to Draft Report: IRM concurs with this recommendation. IRM will codify the necessary changes to applicable policy and procedures and work to incorporate these changes into current FAM/FAH guidance. In the interim, IRM will work to publish an ALDAC that will provide interim guidance to the Department until such time that the FAM/FAH updates occur.

(U) Recommendation 7: OIG recommends that the Bureau of Information Resource Management develop and implement a corrective action plan that addresses how the Department will comply with Department policy on the Systems Authorization Process. The corrective action plan should identify the root cause of compliance failures, action steps to resolve such compliance failures, improvement benchmarks and a timeframe for completion, and an escalation process to hold system owners accountable.

(U) Management Response to Draft Report:

IRM concurs with this recommendation and will develop the necessary corrective action plans, incorporating all of the OIG's recommendation in said plan.

APPENDIX C: BUREAU OF CONSULAR AFFAIRS RESPONSE



United States Department of State

Bureau of Consular Affairs
Washington, D.C. 20520

UNCLASSIFIED

August 2, 2017

INFORMATION MEMO FOR NORMAN P. BROWN - OIG/AUD

FROM: CA – Karen Christensen

SUBJECT: OIG Draft Report on Audit of the Bureau of Consular Affairs, Office of Consular Systems and Technology, Administration of Selected Information Technology Contracts

Thank you for the opportunity to review the draft Management Assistant Report: The Process to Authorize and Track Information Technology Systems Needs. The Bureau of Consular Affairs recommends removing the elements referring to CA systems from the final report, since both systems referenced currently have valid Authorities to Operate. In support of this recommendation, CA submits the below responses with details on the specific actions taken for the two recommendations.

Recommendation 3: OIG recommends that the Bureau of Consular Affairs, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Consular Consolidated Database.

CA Response: The Bureau of Consular Affairs, Office of Consular Systems and Technology (CA/CST) completed a Systems Authorization Process for the Consular Consolidated Database in July 2017 (Tab 1). Because CA/CST has an ATO in place, we respectfully request that recommendation 3 be removed prior to the publication of the final report.

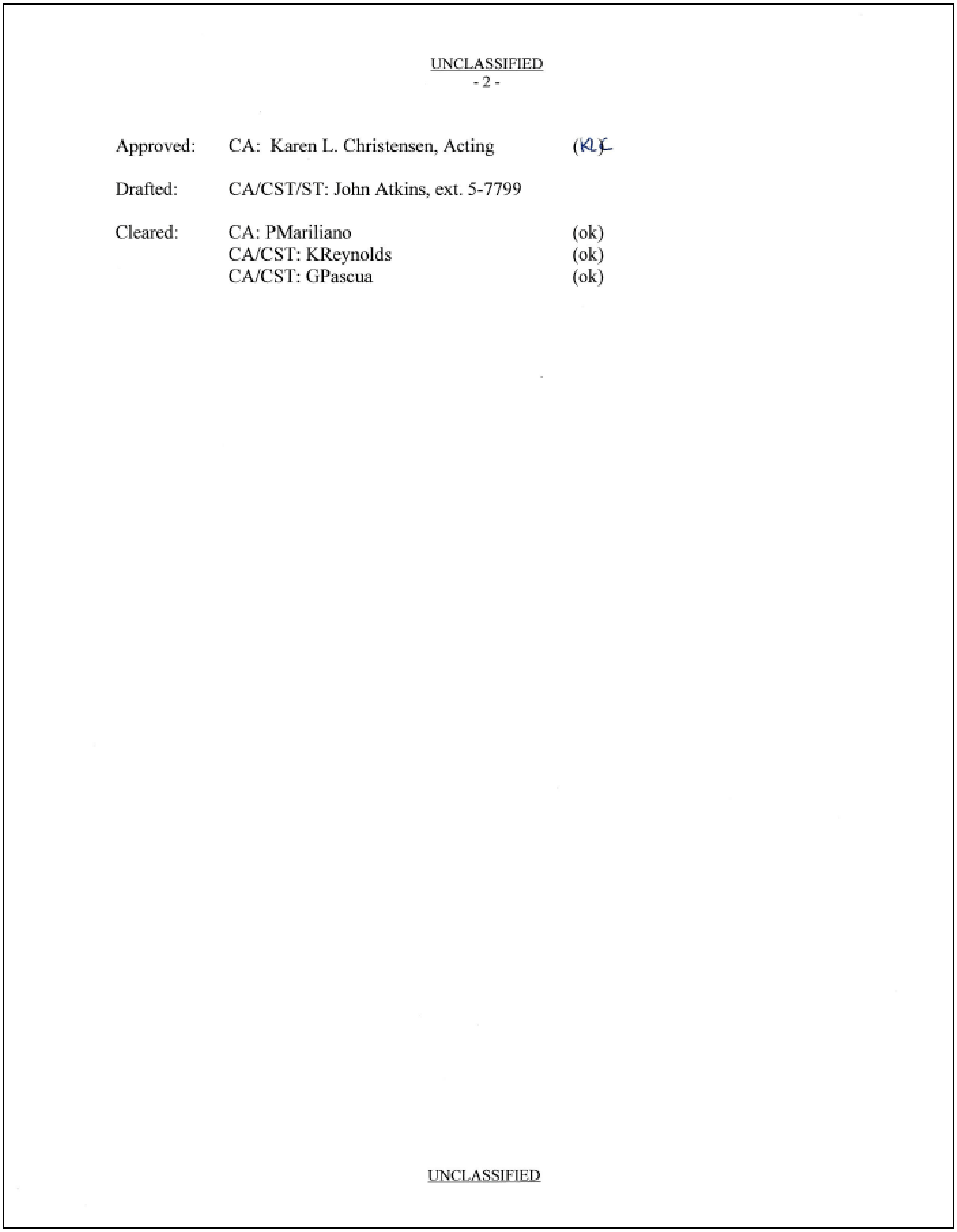
Recommendation 4: OIG recommends that the Bureau of Consular Affairs, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Passport Information Electronic Records System.

CA Response: The Passport Information Electronic Records System (PIERS) is listed as a subcomponent in the attached Passport Application Management System (PAMS) ATO (Tab 2). While this ATO expired, we subsequently implemented an extension in May 2017 which covers all five subcomponents (MIS; PDITS; PIERS; PLOTS; and UMWS) extending the ATO expiration until July 31, 2019 (Tab 3). This extension satisfies the Systems Authorization Process requirement of recommendation 4 and we respectfully request this recommendation be removed prior to the final report submission.

Attachments:

Tab 1 - CCD ATO Memo signed July 2017
Tab 2 - PAMS ATO Memo signed July 2016
Tab 3 - PAMS extension Memo signed May 2017

UNCLASSIFIED



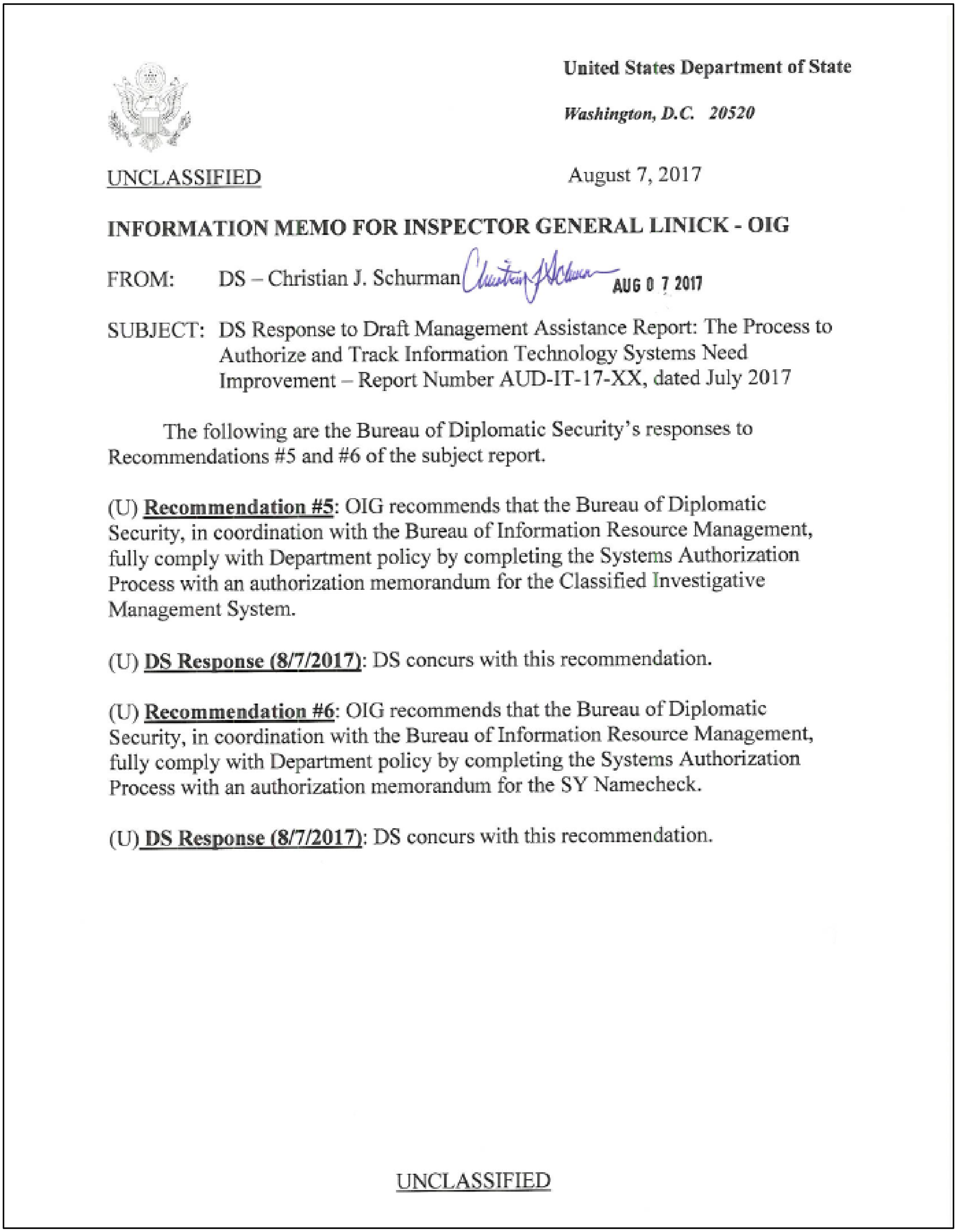
UNCLASSIFIED
- 2 -

Approved:	CA: Karen L. Christensen, Acting	(KLC
Drafted:	CA/CST/ST: John Atkins, ext. 5-7799	
Cleared:	CA: PMariliano	(ok)
	CA/CST: KReynolds	(ok)
	CA/CST: GPascua	(ok)

UNCLASSIFIED

Attachments and tabs are available upon request, consistent with applicable law.

APPENDIX D: BUREAU OF DIPLOMATIC SECURITY RESPONSE



United States Department of State

Washington, D.C. 20520

UNCLASSIFIED

August 7, 2017

INFORMATION MEMO FOR INSPECTOR GENERAL LINICK - OIG

FROM: DS – Christian J. Schurman AUG 0 7 2017

SUBJECT: DS Response to Draft Management Assistance Report: The Process to Authorize and Track Information Technology Systems Need Improvement – Report Number AUD-IT-17-XX, dated July 2017

The following are the Bureau of Diplomatic Security's responses to Recommendations #5 and #6 of the subject report.

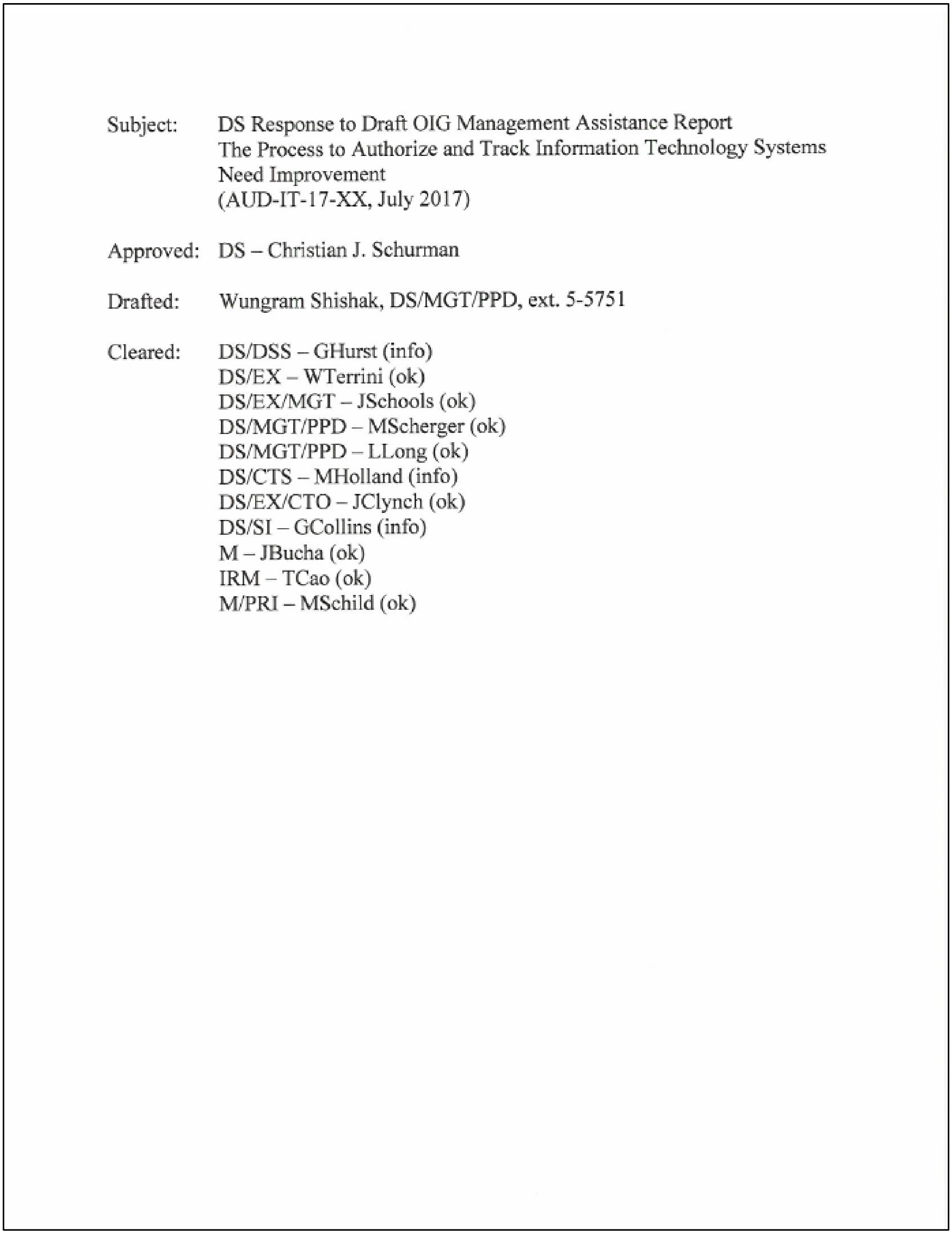
(U) **Recommendation #5**: OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the Classified Investigative Management System.

(U) **DS Response (8/7/2017)**: DS concurs with this recommendation.

(U) **Recommendation #6**: OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Information Resource Management, fully comply with Department policy by completing the Systems Authorization Process with an authorization memorandum for the SY Namecheck.

(U) **DS Response (8/7/2017)**: DS concurs with this recommendation.

UNCLASSIFIED



Subject: DS Response to Draft OIG Management Assistance Report
The Process to Authorize and Track Information Technology Systems
Need Improvement
(AUD-IT-17-XX, July 2017)

Approved: DS – Christian J. Schurman

Drafted: Wungram Shishak, DS/MGT/PPD, ext. 5-5751

Cleared: DS/DSS – GHurst (info)
DS/EX – WTerrini (ok)
DS/EX/MGT – JSchools (ok)
DS/MGT/PPD – MScherger (ok)
DS/MGT/PPD – LLong (ok)
DS/CTS – MHolland (info)
DS/EX/CTO – JClynch (ok)
DS/SI – GCollins (info)
M – JBucha (ok)
IRM – TCao (ok)
M/PRI – MSchild (ok)

OIG AUDIT TEAM MEMBERS

Jerry Rainwaters, Director
Information Technology Division
Office of Audits

Aja Charity, Audit Manager
Information Technology Division
Office of Audits

Nikiya Knight, Senior Auditor
Information Technology Division
Office of Audits

Ebony Mahoney, Senior Auditor
Information Technology Division
Office of Audits

Willie Thomas, Senior Auditor
Information Technology Division
Office of Audits

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
HOTLINE@stateoig.gov
If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:
WPEAOmbuds@stateoig.gov