



UNITED STATES DEPARTMENT OF STATE  
AND THE BROADCASTING BOARD OF GOVERNORS  
*OFFICE OF INSPECTOR GENERAL*

---

ISP-I-13-38

Office of Inspections

July 2013

---

## Inspection of the Bureau of Information Resource Management, Office of Information Assurance

---

~~**IMPORTANT NOTICE:** This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies of organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

---

## **PURPOSE, SCOPE, AND METHODOLOGY OF THE INSPECTION**

This inspection was conducted in accordance with the Quality Standards for Inspection and Evaluation, as issued in 2011 by the Council of the Inspectors General on Integrity and Efficiency, and the Inspector's Handbook, as issued by the Office of Inspector General for the U.S. Department of State (Department) and the Broadcasting Board of Governors (BBG).

### **PURPOSE AND SCOPE**

The Office of Inspections provides the Secretary of State, the Chairman of the BBG, and Congress with systematic and independent evaluations of the operations of the Department and the BBG. Inspections cover three broad areas, consistent with Section 209 of the Foreign Service Act of 1980:

- **Policy Implementation:** whether policy goals and objectives are being effectively achieved; whether U.S. interests are being accurately and effectively represented; and whether all elements of an office or mission are being adequately coordinated.
- **Resource Management:** whether resources are being used and managed with maximum efficiency, effectiveness, and economy and whether financial transactions and accounts are properly conducted, maintained, and reported.
- **Management Controls:** whether the administration of activities and operations meets the requirements of applicable laws and regulations; whether internal management controls have been instituted to ensure quality of performance and reduce the likelihood of mismanagement; whether instances of fraud, waste, or abuse exist; and whether adequate steps for detection, correction, and prevention have been taken.

### **METHODOLOGY**

In conducting this inspection, the inspectors: reviewed pertinent records; as appropriate, circulated, reviewed, and compiled the results of survey instruments; conducted on-site interviews; and reviewed the substance of the report and its findings and recommendations with offices, individuals, organizations, and activities affected by this review.



United States Department of State  
and the Broadcasting Board of Governors

*Office of Inspector General*

## **PREFACE**

This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

This report is the result of an assessment of the strengths and weaknesses of the office, post, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The recommendations therein have been developed on the basis of the best knowledge available to the OIG and, as appropriate, have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "H. W. Geisel". The signature is fluid and cursive, written in a professional style.

Harold W. Geisel  
Deputy Inspector General

## Table of Contents

Key Judgments	1
Context	2
Executive Direction	3
The Information Assurance Role in the Department of State	3
Management Direction and Leadership	4
Program Implementation	7
Policy and Outreach	7
Information Systems Security Officer Program	9
Certification and Accreditation Program	10
iPost Development	15
Content Management	15
Resource Management	17
Budget and Funding	17
Contract Management	17
Inventory Management	22
Training	22
Equal Employment Opportunity	22
Performance Plans and Employee Appraisals	23
Orientation for Incoming Personnel	23
Physical Security	23
List of Recommendations	25
List of Informal Recommendations	28
Principal Officials	29
Abbreviations	30

## Key Judgments

- The Bureau of Information Resource Management, Office of Information Assurance (IRM/IA) was established to address the information security requirements outlined in Title III of the E-Government Act of 2002. The office does not fulfill all those requirements. The majority of the required functions are performed by Department of State (Department) offices other than IRM/IA.
- The current workload of IRM/IA does not justify its organizational structure, resources, or status as an IRM directorate.
- The mishandling of the certification and accreditation (C&A) process and contract by IRM/IA, including development of tools and guidance and reviews of C&A packages has contributed to expired authorizations to operate 52 of the Department's 309 systems.
- No single Department bureau has full responsibility for the information systems security officer (ISSO) program. Both IRM and the Bureau of Diplomatic Security (DS) directly or indirectly support the ISSO program, resulting in confusion among personnel on requirements and guidance. The involvement of both bureaus also wastes personnel resources.
- IRM/IA lacks adequate management controls and procedures to monitor its contracts, task orders, and blanket purchase agreements, which have an approximate value of \$79 million.
- IRM/IA has no mission statement and is not engaged in strategic planning.

All findings and recommendations in this report are based on conditions observed during the on-site review and the standards and policies then in effect. The report does not comment at length on areas where the Office of Inspector General (OIG) team did not identify problems that need to be corrected.

The inspection took place in Washington, DC, between February 4 and March 22, 2013.

[Redacted] (b) (6)

conducted the inspection.

## Context

IA is one of three IRM directorates. IRM/IA, headed by the Department's chief information security officer (CISO), was created in August 2003 in response to requirements set forth in Title III of the E-Government Act of 2002 and the Federal Information Security Management Act of 2002 (FISMA). The CISO is the Department's senior information security official as delineated in the legislation.

IRM/IA is responsible for the Department's cyber security program; information assurance policies, standards, and guidelines; and compliance with National Security directives. The key programs of IRM/IA include cyber security management, which is comprised of policy development, risk management, systems authorizations, performance measures, and annual reporting for FISMA. IRM/IA collaborates with DS on information security responsibilities.

IRM/IA has three divisions. The System Authorization Division delivers information security services to customers for C&A compliance and system monitoring and handles contract management. The Global Oversight Division assists with the Department's ISSO program by supporting domestic and overseas personnel in the performance of their responsibilities. The Policy, Liaison, and Reporting Division provides information security policy and liaison support for IRM/IA. This division also coordinates the annual FISMA submissions to the Office of Management and Budget.

The role of IRM/IA in information security has evolved in response to advancements in technology and the introduction of new Federal legislation and directives. While the creation of the office was prompted by FISMA, guidance and directives from the Federal Chief Information Office Council, the Office of Management and Budget, and the National Institute of Standards and Technology help shape priorities and information security activities. The response of IRM/IA to these evolving requirements is critical to the Department's information security posture.

IRM/IA staff is comprised of 22 full-time employees and 36 contract employees, though this number fluctuates as perceived needs change. Funding for IRM/IA activities is \$5.9 million per year from FYs 2011–13. The annual operating budget for IRM/IA in FY 2013 is approximately \$10 million, with other funds coming from reimbursements and internal bureau transfers. For FY 2014 planning, the Chief Information Officer increased the IRM/IA budget request by an additional \$8 million to support specific Department initiatives. IRM/IA is supported by five procurement vehicles with a total value of more than \$79 million. IRM/IA is also supported through the Vanguard 2.2.1 contract—a series of the overall Vanguard performance-based contract valued at \$2.5 billion.

## Executive Direction

### The Information Assurance Role in the Department of State

IRM/IA was established to address the information security requirements outlined in Title III of the E-Government Act of 2002; however, IRM/IA is not the focal point for all Department information assurance<sup>1</sup> functions. The majority of functions are performed by other offices. IRM/IA is not doing enough and is potentially leaving Department systems vulnerable. IRM/IA has conceded that other Department elements have a greater role in information security, diminishing the relevance of IRM/IA.

DS has several offices handling information security elements,<sup>2</sup> including information technology (IT) personnel monitoring information security incidents, assessing cyber security, managing technical security of facilities, and performing network management, as well as developing information security policies and standards for IT personnel. Within other IRM offices,<sup>3</sup> personnel are responsible for the management and oversight of the Department's information systems, which includes the Department's unclassified and classified networks. IRM IT personnel monitor network and infrastructure for cyber attacks and risk measures; provide operation and maintenance support for all IT infrastructure systems and equipment; and establish policies, processes, and procedures for consolidated bureaus on desktop security guidelines. In addition, the Bureau of Intelligence and Research handles all aspects of information security for the Department's intelligence systems. The Office of the Coordinator for Cyber Issues located in the Secretary of State's executive office was recently created to coordinate and manage cyber security issues within one office as required, both within the U.S. Government and with diplomatic engagements worldwide.

IRM/IA performs a limited number of information assurance functions, does not have a lead role in most of the functions it does perform and, for the most part, only compiles information generated by others. For example, IRM/IA is tasked with overseeing the ISSO program, but is not the principal office where ISSO personnel overseas seek information and guidance. Several ISSOs surveyed by OIG were not even aware of the involvement of IRM/IA. IRM/IA is also tasked to be the Department's lead in C&A<sup>4</sup> activities, yet many bureaus and offices complete necessary C&A assessments and documents without the involvement of IRM/IA. More significantly, IRM/IA does not have the lead for the most important C&A effort in the Department—the OpenNet network. That task is handled by IRM's Enterprise Network Management Office.

---

<sup>1</sup> According to the National Institute of Standards and Technology, information assurance is a measure of confidence that the security features and architecture of an information system accurately enforces the security policy and is composed of the degree of availability, confidentiality, accountability, and integrity required.

<sup>2</sup> DS offices include the Office of Computer Security, the Office of Information Security, the Computer Investigation and Forensics divisions, and the Office of Security Technology.

<sup>3</sup> IRM offices include the Enterprise Network Management Office, the Office of Information Technology Infrastructure, and Operational Support division.

<sup>4</sup> According to the National Institute of Standards and Technology, C&A is the comprehensive assessment and approval of the security controls of an information system to determine the extent to which the controls are implemented correctly, operating as intended, and meeting security requirements. Traditional C&A is performed every 3 years or when a significant change is made. Continuous monitoring is performed on an ongoing basis; however, it does not replace the C&A requirement.

In light of the lack of active involvement in many of its stated responsibilities, the proposed IRM/IA office realignment for an additional deputy position and one more division, as well as the need for some of the current divisions, are not justified by the current level of work being performed. The possibility of duplicative functions occurring between IRM/IA and other Department elements is likely. The realignment package is currently being reviewed by the Bureau of Human Resources, Office of Resource Management and Organizational Analysis, and the package does not provide strong support for approving the realignment proposal. It does not include most of the documentation the Office of Resource Management and Organizational Analysis requires, which includes an explanation of how the proposed organization will meet the Department's management goals, a crosswalk of changes occurring to staff functions, or a communications plan outlining how IRM/IA is planning to solicit views and input from stakeholders. A further analysis of the organization, responsibilities, and workload of IRM/IA is necessary to provide the Department with reassurance that the current and proposed resources are justified prior to any approval of office realignment.

IRM/IA indicated that their management met with the Office of Resource Management and Organizational Analysis twice to discuss the organizational assessment since the completion of OIG's inspection. An assessment study is scheduled to begin in June 2013 with tentative completion by September 2013.

**Recommendation 1:** The Bureau of Human Resources should direct the Office of Resource Management and Organizational Analysis to perform an organization assessment of the Bureau of Information Resource Management, Office of Information Assurance, including a workforce and workload balance analysis and a review of similar functions that are being performed by other offices in the Department of State. (Action: DGHR)

### **Management Direction and Leadership**

The current CISO arrived at the end of September 2012 and with his arrival the atmosphere in the office has improved. He has focused on rebuilding relationships both internally and externally with other IRM and Department offices. However, attention is needed to define the office's mission and goals and outline its strategic vision.

### ***Mission and Goals***

The CISO has not addressed critical management issues. IRM/IA does not have a mission statement outlining a vision for the office and specific goals for each of its three divisions. In fact, the CISO was in the process of drafting a mission statement at the end of the inspection. No document provides a clear connection between the work of IRM/IA and the high-level goals outlined by the Chief Information Officer in the Department's IT Strategic Plan for FYs 2011–13. The CISO has not provided division chiefs with priorities based on defined goals. As a result, the staff is not proactive in meeting information security requirements.

The CISO held nine staff meetings in the first 6 months after his arrival. IRM/IA staff commented that those meetings normally do not provide clarity on what the CISO considers to be office priorities. Many staff commented that they are unaware of the CISO's activities in general and are unable to obtain those answers since he is not seen regularly in the office. The

creation of a mission statement and office goals would assist staff in understanding their work requirements and priorities and improve financial and resource planning.

**Recommendation 2:** The Bureau of Information Resource Management should develop a written mission statement for the Office of Information Assurance that includes short-term and long-term priorities and goals for the office and each division. (Action: IRM)

### *Strategic Planning*

IRM/IA is not engaged with IT strategic planning in the Department. The Department's Quadrennial Diplomacy and Development Review (QDDR) process stresses the importance of multiyear strategic planning Departmentwide as a way to assess policy priorities, anticipate changing requirements, and justify resource requirements. IRM produces 3-year strategic and tactical plans with the QDDR goals in mind. With increased concerns about cyber security in the Department and the Federal government, the importance for the Department to create strategic documents that reflect broad collaboration is heightened; however, IRM/IA has not actively engaged in strategic planning efforts within the Department. These strategic planning efforts should include participating in strategy meetings or collaborating with the IRM Strategic Planning Office—the central office of IRM that facilitates management decisions for planning purposes.

The current Department IT Strategic Plan for FYs 2011–13 contains little mention of information assurance functions. Nor is information assurance addressed prominently in the IRM Strategic Plan for 2014–2016. While there are references in these plans to the importance of protecting the Department's worldwide IT network and information assets, the strategy and crosswalk for addressing these factors with the involvement of IRM/IA is not detailed in the strategic or tactical plans' goals and objectives.

IRM/IA needs to engage with all offices in the Department that perform or are engaged in information security functions for strategic planning purposes. For example, IRM/IA should coordinate its strategic planning with DS as many of the security functions are handled by DS programs and personnel. One of the three goals listed in the DS FY 2013 Bureau Strategic and Resource Plan<sup>5</sup> is to “securely enable the Department's global cyber operations and information assets.” The goal includes three performance indicators and targets related to systems operations, capability to identify and address threats, and training on cyber awareness. The actions of DS illustrate more consideration and preparation than IRM/IA, which by statute is the lead office for information assurance and security. Mission clarity and resource alignment should be reflected in the work being performed by both bureaus in order to effectively manage resources and funding requirements.

**Recommendation 3:** The Bureau of Information Resource Management should revise its Department of State Information Technology Strategic Plan to include the Office of Information Assurance activities. (Action: IRM)

---

<sup>5</sup> In December 2011, the Department issued 11 STATE 124737, which discontinued the Bureau Strategic and Resource Plan. The Bureau Resource Request (three-year strategic plans, with shorter annual resource requests) replaces the Bureau Strategic and Resource Plan beginning with the FY 2014 budget cycle.

IRM/IA does not have an office strategic plan. There is no evidence of IRM/IA management engaging in a comprehensive strategic review to assess its current capabilities and future needs. The CISO and his division chiefs have not reviewed operations to determine what information assurance and security functions they are required to perform or are currently handling based on statutory requirements. There is no record of IRM management discussing how the office is performing those functions and whether sufficient resources and funding is available to meet future needs.

The information assurance landscape is constantly changing as the U.S. Government continues to address cyber security concerns involving government operations and critical infrastructure. IRM/IA, under the direction of the CISO, needs to participate in these initiatives within the Department. Proper strategic planning will assist in that endeavor.

***Informal Recommendation 1:*** The Bureau of Information Resource Management should require the Office of Information Assurance to develop an office strategic plan that aligns with its mission and goals and with the Department of State's Information Technology Strategic Plan.

## Program Implementation

### Policy and Outreach

Policy and outreach in IRM/IA has been inconsistent and ineffective. IRM/IA does not update Department regulations—the *Foreign Affairs Manual* (FAM) and *Foreign Affairs Handbook* (FAH)—to reflect current information security responsibilities among personnel or to show alignment with statutory requirements. Collaboration between IRM/IA and other Department offices performing information security functions is very limited. Internal and external outreach efforts are neither extensive nor do they include any internal mechanism by IRM/IA management to collaborate and share information gathered during outreach activities with its divisions that perform the respective functions.

### *Information Technology Policy*

The CISO is charged with developing and maintaining the Department's information security policies per statutory requirements set forth in FISMA. These include developing, implementing, and maintaining an agencywide information security program plan. This responsibility is coordinated with DS, which handles physical protection and implementation of operational information security programs. IT policies developed by IRM are addressed in 5 FAM and 5 FAH regulations, while IT policies managed by DS are outlined in 12 FAM and 12 FAH regulations. The Policy, Liaison, and Reporting Division was established within IRM/IA to support the CISO in developing Departmentwide information security policies and plans.

Many portions of IRM 5 FAM and 5 FAH regulations have not been updated since February 2007. This is a concern because Department IT personnel obtain guidance and instructions from these specific FAM and FAH regulations to administer their information security responsibilities. Further, many of these FAM and FAH regulations stem from legislation and guidelines outlined by Congress, the White House, the National Institute of Standards and Technology, and the Office of Management and Budget, to whom the Department must report regarding its information security posture. The Department is reporting on its information security posture using outdated requirements.

IRM/IA is making changes to FAM and FAH regulations with little coordination and collaboration with other offices within the Department that play a role in information security functions. These offices include other IRM offices, DS offices, the Bureau of Intelligence and Research, and the Office of the Coordinator for Cyber Issues. Representatives from these offices informed the OIG team that narrative input and clearances were not sought by IRM/IA for IT FAM and FAH changes. For example, the language in 12 FAM that is handled by DS does not match language in 5 FAM that is handled by IRM. Terminology for IT functions and personnel are often outdated.

Additionally, IRM FAM and FAH policies do not mention the latest technologies and efforts within the Department. For example, there is little mention and guidance for handling social media. The limited guidance in 5 FAM was written in 2010 and is outdated. There is no mention of cloud computing in 5 FAM, which is surprising considering that cloud computing is

described as a strategic goal for IRM in its IT Strategic Plan. These types of policy development are the responsibility of IRM/IA, and more importantly the CISO, per statutory requirements.

IRM/IA management indicated that it is working with DS and IRM's Governance, Resource, and Performance Management Office to create new policies and update existing 5 FAM policies related to information and cyber security. The office anticipates the process should be completed by February 2014.

**Recommendation 4:** The Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, should direct the Office of Information Assurance to update Volume 5 of the *Foreign Affairs Manual* and *Foreign Affairs Handbook*. (Action: IRM, in coordination with DS)

**Recommendation 5:** The Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, should implement a clearance process for revisions and updates to the *Foreign Affairs Manual* and *Foreign Affairs Handbook* that includes the review and approval of both bureaus. (Action: IRM, in coordination with DS)

Detailed guidance on IT security exceptions in FAM and FAH regulations is needed. Currently, the language in 12 FAM 600 and 5 FAM 600 does not provide clarity on what constitutes an IT security exception and what procedures should be followed for requesting approval. The only tool available is an informal procedural outline on the IRM/IA Web site.

The Global Oversight Division coordinates and tracks all IT security exceptions. Exceptions to DS policies contained in 12 FAM are sent from the Global Oversight Division to the Office of Computer Security in DS for review prior to being forwarded to the CISO for approval. The 5 FAM exceptions are maintained within IRM/IA for review and approval. The division tracks all exceptions through a SharePoint library, which prompts an automatic notice for both the post and IRM/IA regarding expiring approved exceptions.

A review of recent IT security exceptions identified inconsistent procedures in the requests from the originator. Further, results of the OIG survey sent to domestic and overseas ISSOs showed confusion among a large amount of respondents regarding IT security exceptions. More detailed policies on IT security exceptions are critical for the Department's compliance with IT security requirements.

IRM/IA management informed the OIG team that they are working closely with DS to update the relevant 5 FAM and 12 FAM sections. Further, IRM/IA officials agree that it is imperative for their staff and DS to update the documents in a parallel manner to avoid conflict and confusion. IRM/IA anticipates the targeted completion to be June 2014.

**Recommendation 6:** The Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, should establish *Foreign Affairs Manual* and *Foreign Affairs Handbook* policies on information technology security exceptions, including descriptions of types of exceptions and procedures for requesting waivers. (Action: IRM, in coordination with DS)

### *Outreach Efforts*

IRM/IA management needs to share information gathered from outreach efforts with its staff and participate regularly in Departmentwide IT working groups. Under the previous CISO, the office did not engage in outreach activities; however, the current CISO is focusing on them. The CISO maintains regular contact with the Office of Management and Budget, the Department of Homeland Security, the U.S. Agency for International Development, and the Office of the Director of National Intelligence. During the inspection, a meeting was also held with other government CISOs to enhance collaboration. The Policy, Liaison, and Reporting Division, which is responsible for administering outreach activities for IRM/IA, serves as the liaison between IRM/IA and system owners.

IRM/IA management is focused on building relationships outside the Department; however, that same focus is also needed on its outreach activities within the Department—such as with DS. IRM/IA co-chairs various working groups with DS but does not send participants to attend these meetings. For example, both bureaus jointly host the Awareness, Training, Education, and Professionalism working group responsible for developing a training plan for cyber security. IRM/IA has not attended the working group meetings for some time based on attendance records. Further, IRM/IA has not participated regularly in Cyber Security Policy Development working group meetings, and therefore is not involved in policy updates and changes to Department regulations based on cyber security matters. IRM/IA management needs to strongly encourage its staff to maintain regular contact with peers and attend Department meetings.

IRM/IA management needs to share information gathered from Department meetings with its staff to ensure employees have the most relevant and current information to perform their tasks. IRM/IA is not using any collaborative tools to share information. As a result, IRM/IA staff members have a mixed level of awareness and understanding on their relevant projects and Department efforts.

**Recommendation 7:** The Bureau of Information Resource Management should require the Office of Information Assurance to participate regularly in Departmentwide information technology working group meetings and share learned information from such meetings with its staff. (Action: IRM)

### **Information Systems Security Officer Program**

No single Department bureau has full ownership of the ISSO program. Both IRM and DS directly or indirectly support the ISSO program, resulting in confusion among personnel on requirements and guidance. The involvement of both bureaus also wastes personnel resources. ISSOs are responsible for managing information security at each office or post. At overseas posts the function is typically performed as collateral duty and includes implementing information security policies and guidelines and ensuring that systems and networks are operating at acceptable levels of risk. Domestically, the position is often full time and typically includes special responsibilities involving bureau-specific applications.

DS has taken a more active role in the ISSO program. The DS Security Engineering and Computer Security Training Division provides ISSO training to IT personnel, which includes

compiling course content and interacting with the Foreign Service Institute on class attendance. DS conducts and funds ISSO training either at selected posts worldwide or at its Washington, DC, training center and also manages the Cyber Security Awareness program for all Department personnel. DS personnel developed the ISSO checklist used by IT personnel to fulfill the requirements set forth by the Department in performing ISSO-related responsibilities. The checklist is an important tool to identify and prioritize how ISSOs should implement their responsibilities and is the cornerstone for the ISSO training course. Additionally, DS has an active Web resource managed by the Office of Computer Security for ISSOs to seek advice on IT security matters. Department policy covering ISSO duties is also more detailed in 12 FAM and FAH regulations that are managed by DS than in 5 FAM and FAH regulations handled by IRM.

Within IRM, IT personnel at regional information management centers provide ISSOs with operational guidance and support. IRM also has a separate program office in its Security Management branch to support ISSO functions for IT-consolidated domestic bureaus. The branch establishes policies, processes, and procedures for consolidated bureaus' compliance with desktop security guidelines and monitors systems for risks and security measures.

In addition, the Global Oversight Division in IRM/IA has an informational support role. The division maintains an electronic educational library that contains templates, Federal and Department guidance, and accreditation reports and tracks exceptions to IT security policy. The division has two email addresses to assist ISSOs. The response time by the Global Oversight Division varies depending on which email address is used and often by the rank of the individual requesting assistance. An ISSO blog was being coordinated by the Global Oversight Division, but it is no longer active. Currently, an ISSO discussion board is used to promote dialogue among ISSOs.

The division of responsibilities between DS and IRM, including policy development and implementation, training, reporting guidance, and information sharing, reduces accountability for IT security management and increases ambiguity among personnel. The consolidation of the ISSO program within one bureau would enable the Department to better align its technical expertise, personnel, and financial resources to support this vital information security function.

**Recommendation 8:** The Office of the Under Secretary for Management, in coordination with the Bureaus of Diplomatic Security and Information Resource Management, should assign responsibility of the information systems security officer program to a single bureau. (Action M/PRI, in coordination with DS and IRM)

### **Certification and Accreditation Program**

The CISO has directed the System Authorization Division to take the lead in the Department's C&A activities, yet it does not have a leadership role in the C&A process. Under the previous CISO, the Department made a concerted effort to devote resources to move away from traditional C&A activities and reporting to continuous monitoring, which would continuously monitor the security controls implemented within systems. Proponents of continuous monitoring believe it sufficiently meets requirements for systems authorizations every 3 years, as well as requirements to report significant systems deficiencies to the Office of Management and Budget. After the departure of the previous CISO, the Chief Information

Officer at that time decided to revert to traditional C&A reporting. However, at that point the Department had diverted significant resources away from C&A reporting, and as a result, a formal C&A has not been completed for the primary general support systems for the Department (OpenNet and ClassNet) since 2007.

The incomplete transition from traditional C&A reporting to continuous monitoring has created uncertainty about which direction the Department will adopt and who will be responsible. Survey responses from system owners indicate that many bureaus and offices are completing assessments and documents without the involvement of IRM/IA, with a few bureaus acquiring their own contract support for their C&A work. Further, the most important C&A activity for the Department—the OpenNet network—is done outside of IRM/IA, with IRM/IA only attending meetings. Employees in the System Authorization Division, which includes contract staff via the Vanguard 2.2.1 scope, are handling few C&A activities. These C&A activities include the development of C&A tools and guidance and review of C&A packages once submitted by the system owners for approval. However, there are issues for each of these activities performed by IRM/IA, which are detailed below.

### ***Tools and Guidance***

System owners described IRM/IA tools as difficult to use and not user-friendly. Many commented that the tools would lock up while entering content, requiring information to be reentered. System owners attempted to share their frustrations regarding C&A tools with IRM/IA, but to no avail. This led system owners to research other means to complete C&A activities. One system owner conveyed that her bureau was using a different tool for storing C&A information than the one provided by IRM/IA.

For example, the Plan of Action and Milestones Toolkit was cited as particularly weak. The toolkit is used to track security vulnerabilities as part of the C&A process. It is a stand-alone database only accessible by IRM/IA System Authorization Division staff. System owners are provided with a printed spreadsheet to note by hand any updates. These are then entered by IRM/IA staff, reducing the level of accountability for the system owner. By including manual processes, IRM/IA is contradicting the main reasons to use an electronic means—to reduce paper and improve efficiency. Further, Plan of Action and Milestones Toolkit for multiple systems, which detail security vulnerabilities with the systems and must be protected, are stored improperly by the System Authorization Division. IRM/IA staff is storing information in shared folders on systems operating at lower security classification levels than the information being stored.

System owners also expressed concerns regarding iPost, a database that aggregates information derived from diagnostic tools run by other Department offices. The system owner for iPost is IRM's Enterprise Network Management Office; however, IRM/IA staff promotes its usage, manage its everyday support, and answer questions from the users. The iPost database integrates selected performance, security, and configuration data according to IRM/IA risk measurement criteria to present a single simplified interface. System owners commented that on occasion iPost reported scores lower than they should be. System owners are held accountable for the low scores even after reporting mistakes to IRM/IA. IRM/IA management reported that a change in the criteria used by iPost creates such a situation but sent no Departmentwide notification to inform users of any changes.

The IT Asset Baseline, now known as iMatrix, is another tool used by system owners. The tool is used to record all attributes associated with each Department system, including security classification and funding. System owners are asked to report on each information system within iMatrix and regularly update the data. IRM/IA is responsible for validating the active period for each system and requires each system to have the necessary authorization to operate. However, several reported systems in iMatrix had incorrect information. For example, several systems were shown as having an expired authorization to operate, but in reality the systems had received extensions to continue to operate.

Many system owners cited issues with the guidance provided by IRM/IA for C&A activities and the constant level of changes occurring to templates without any notification or consideration of the ramifications to the entire C&A process. The C&A Toolkit on the IRM/IA Web site is a reference point for system owners to obtain information on the latest changes to templates and guidance. There is no governance process within IRM/IA regarding why, how, or when template changes are made to the C&A Toolkit. During the inspection, the IRM/IA staff was making changes to templates in an ad hoc manner; the staff told the OIG team that ad hoc changes were normal. With frequent changes made to C&A guidance and templates, system owners often proceed with the C&A process and are informed at completion that their package is incorrect. Over 90 percent of C&A packages submitted during the course of the inspection were either incomplete or unusable due to a change that occurred to the guidance without system owners being notified.

IRM/IA management agrees with the need to survey system owners regarding their issues with the C&A tools and plans to issue a survey tool to gather information shortly.

**Recommendation 9:** The Bureau of Information Resource Management should survey system owners on issues they are encountering with certification and accreditation tools and take necessary corrective steps to improve the certification and accreditation tools, guidance, templates, and procedures. (Action: IRM)

**Recommendation 10:** The Bureau of Information Resource Management should develop a control process for changes to certification and accreditation templates and guidance that includes advance notice to system owners of pending changes. (Action: IRM)

### ***Review by Assessors***

C&A packages are reviewed by a group of assessors in the IRM/IA System Authorization Division. These personnel are contractors who perform C&A work under the scope of the Vanguard 2.2.1 contract. Many system owners noted in their OIG survey responses that the level of interaction and review varied with each assessor. Some C&A packages received close scrutiny on all required elements, such as the appropriate level of security categorization for the system and the level of risk assessment performed, while others did not. Some system owners described assessors as lacking an understanding of the C&A process and the Department's operating environment.

The level of review performed by the assessors would benefit from the identification of common security controls for Department systems. Common security controls identify the management, operational, and technical safeguards or countermeasures needed for

Department systems to protect the confidentiality, integrity, and availability of its information. Many Department systems are dependent on parent-child relationships to the Department's primary enterprise general support systems—OpenNet and ClassNet. As a result, many systems submitted for C&A approval by system owners would inherit the same levels of security categorization and controls as the primary system. The use of common security controls allows system owners and the C&A assessors to have a baseline as a starting point to facilitate a more consistent level of review and security for all Department systems. To date, IRM/IA has not taken the necessary steps to identify the common controls for its systems or disseminate this information to the relevant individuals.

IRM/IA management informed the OIG team that their office has taken the lead in the development of unclassified common controls and has been working on the effort for the last 7 months, with anticipated completion by the end of the calendar year.

**Recommendation 11:** The Bureau of Information Resource Management should identify the common security controls for its Department of State systems. (Action: IRM)

**Recommendation 12:** The Bureau of Information Resource Management should document the necessary review steps to be performed by each certification and accreditation assessor. (Action: IRM)

### *Expired Authorizations to Operate*

With the frequent changes to guidance, non-user-friendly tools, and varied degrees of review being performed by assessors, the C&A process managed by IRM/IA is ineffective. As a result, many systems have expired authorizations to operate. Despite being the lead office for information assurance, IRM/IA is only responsible for completing the C&A packages for 56 percent of the Department's 309 systems. The remainder of the C&A packages are handled by DS and the Bureau of Consular Affairs. Of the total number of Department systems requiring C&A, 52 systems currently have expired authorizations to operate. IRM/IA is responsible for 36 of those lapsed systems, which represent 69 percent of the total lapsed systems. Further, the expired authorizations to operate for DS and the Bureau of Consular Affairs are recent occurrences. Delinquent systems under the responsibility of IRM/IA have been operating with expired authorizations, in many cases for 2 years or more.

When questioned, IRM/IA management stated that the responsibility for completing system authorizations is with system owners. System owners have a responsibility to complete the necessary documentation and assessments, but ultimately it is the CISO's responsibility to verify that systems authorizations have been performed on all Department systems in accordance with Title III of the E-Government Act of 2002.

The CISO has discussed plans to conduct a workload analysis of the C&A process to determine whether the requirement to have a C&A review performed every 3 years could be completed more effectively. The CISO is considering splitting the number of Department systems into three equal parts to avoid a flux in the level of work and to ensure that C&A assessors would have a constant flow of work. This could be a viable option after further review; however, the CISO's top priority should be to address expired authorizations to operate and to mitigate any potential security vulnerabilities.

**Recommendation 13:** The Bureau of Information Resource Management should develop an action plan to address all Department of State systems with expired authorizations to operate. (Action: IRM)

***Certification and Accreditation Reimbursements***

IRM/IA does not have an effective process for tracking C&A reimbursements received from bureaus. Department bureaus fund a predetermined amount to IRM/IA for its assistance in performing risk assessments as part of C&A efforts for the bureaus' systems. C&A reimbursement amounts are maintained in the Department's Corporate Budget Allocation Tracking System (CBATS) and an internal spreadsheet maintained by the IRM/IA System Authorization Division.

IRM/IA provided the OIG team with documentation showing C&A reimbursements received for the last 2 fiscal years. The documentation showed that in FY 2012, the CBATS showed a total for C&A reimbursements of \$562,058, while the IRM/IA funding spreadsheet showed a total of \$258,944. For FY 2011, the CBATS showed a total of \$551,490, and the IRM/IA spreadsheet displayed a total of \$2,770,057.

One factor contributing to the difference in C&A reimbursement totals is that IRM/IA includes reimbursements for systems under the Vanguard 2.2.1 contract, which IRM management decided not to include since those systems are covered under the contract cost. Further, no one in IRM/IA is assigned the responsibility to reconcile the C&A reimbursements listed in the CBATS against the IRM/IA funding spreadsheet. Bureaus have also been unable to validate the accuracy of C&A reimbursements reported since IRM/IA no longer provides close-out reports to system owners. Without accurate reporting, IRM/IA cannot guarantee that they are receiving the correct amount for reimbursements, and bureaus may be due refunds for overpayments made for C&A activities.

IRM/IA informed the OIG team in their report comments that the office is in the midst of establishing a process to verify associated C&A costs incurred by system owners. Cost accounting procedures are being developed to ensure system owners are only paying for work directly associated with the cost of completing their C&A tasks. Once the new cost accounting procedures are established, a close-out report will be provided to the systems owners for cost verification.

**Recommendation 14:** The Bureau of Information Resource Management should assign an individual to review and reconcile certification and accreditation reimbursements between the Corporate Budget Allocation Tracking System and the Bureau of Information Resource Management's internal funding spreadsheet. (Action: IRM)

**Recommendation 15:** The Bureau of Information Resource Management should provide system owners with close-out reports for verification of associated certification and accreditation costs. (Action: IRM)

## **iPost Development**

IRM lacks a defined project management methodology for iPost. A project management methodology defines the recommended procedures by which an organization envisions, defines, builds, deploys, operates, and maintains its systems and applications. The absence of such a methodology has resulted in a lack of reliability of tools used by Department personnel for reporting systems and their associated security measures.

For example, iPost is owned by IRM's Enterprise Network Management Office, but its everyday management and support to users is handled by IRM/IA. The tool has been widely promoted in the Department and among other Federal agencies. iPost was recognized with numerous government recognitions and awards.<sup>6</sup> Nevertheless, the OIG team found no project management documentation or evidence of the office following any project management methodology for the development and maintenance of iPost during its life cycle. IRM had no planning documents or budget information for iPost. There was no source code documented to illustrate how information is aggregated to reflect the scores shown and reported by the tool. IRM management was unable to explain how the tool was developed and what network and security information is actually being collected and used. IRM/IA is in the process of reviewing iPost in hopes of understanding its origin. Additionally, iPost is one of the Department's systems that does not have a current authorization to operate. The CISO hopes to understand what information is collected and used for iPost scores and obtain a better understanding of the source code so that future program changes can be made.

**Recommendation 16:** The Bureau of Information Resource Management should develop project management documentation for iPost. (Action: IRM)

## **Content Management**

Content organization and management of the IRM/IA Web site and shared network needs to be improved. The IRM/IA Web site contains outdated information and reference materials. Toolkits do not include the current version of templates required to be used by system owners or references to current guidelines. Additionally, the IRM/IA Web site has no background information for visitors that explains the functions performed by IRM/IA and what role the office plays in the Department. There is no posted organization chart with details on staff, management, or the new CISO. Additionally, the IRM/IA shared network contains many items that are not organized in a logical and easy to use manner. The shared drive contains more than 240 folders as well as additional random documents. The labeling of the folders is not detailed enough to provide content clarity. Many folders contained documents more than 5 years old.

The lack of a content manager and defined processes have resulted in IRM/IA staff being unable to locate information in a timely manner, including documents pertaining to C&A

---

<sup>6</sup> The Department's Risk Scoring program, which is implemented via iPost, was awarded the National Security Agency's 2009 Frank B. Rowlett Award for Organizational Achievement, recognizing the Department for making a significant contribution to the improvement of national information systems security and operational information assurance readiness. The System Administration, Networking, and Security Institute awarded the Office of the Chief Information Officer in 2011 the U.S. National Cybersecurity Innovation Award for significantly improving the effectiveness of the nation's cyber security by creating, deploying, and sharing the iPost's Risk Scoring program.

**~~SENSITIVE BUT UNCLASSIFIED~~**

activities and contract management. Currently, one contractor maintains the IRM/IA Web site, but the individual does not request content updates from the divisions or review the material on a regular basis. Also, this individual does not oversee the shared network and its contents. An assigned content manager and defined process would improve content relevancy, timeliness, and accuracy.

**Recommendation 17:** The Bureau of Information Resource Management should assign a content manager and define a content management process for managing the content on its Office of Information Assurance Web site and shared network. (Action: IRM)

## Resource Management

### Budget and Funding

The leadership of IRM/IA has not given sufficient attention to assessing and addressing its operationally mandated requirements for information assurance, leading to a widespread belief among staff that the office does not have enough financial resources to meet its needs. IRM/IA has not carried out its budget planning effectively in recent years. The OIG team could not validate whether IRM/IA has not been able to meet priorities since the office has not defined any priorities. The lack of adequate involvement in budget formulation by IRM/IA has led to the office having minimal funds available for staff travel and training.

The baseline budget figure for IRM/IA operations are funded out of Diplomatic and Consular Programs and Worldwide Security Protection program funding, which has remained at \$5.9 million for FYs 2011–13. The overall funding for IRM/IA is approximately \$10 million per year when additional funds from reimbursements and internal IRM transfers are included. For FY 2014, the previous Chief Information Officer directed an additional \$8 million to IRM/IA to support C&A initiatives, continuous monitoring, and controls needed for safeguarding classified information.

IRM/IA did not participate in the IRM budget formulation process in the past, and no progress has been made under the new CISO. IRM/IA did not participate in budget request calls for FY 2014. Also, there is no evidence of collaboration by IRM/IA with other IRM offices or other Department entities for analyzing and capturing the broader budgetary requirements to manage the information security activities of the Department.

As part of the budget formulation for FY 2015, IRM plans to use a zero-base budgeting approach. This approach will require all of IRM to build requirements from the ground up to include specific justifications, objectives, assumptions, proposed performance targets, and indicators. It will include accomplishments for the prior 3 fiscal years, cost savings and avoidance projections, and a focus on identified risks. IRM management believes the zero-base approach will more closely align budget planning with strategic and resource planning under the QDDR process and with guidance from the Bureau of Budget and Planning. IRM/IA can play a vital role in helping ensure that information security requirements are met with a zero-base budgeting approach. Most importantly, IRM/IA can ensure sufficient resources are available to carry out an effective information security program.

**Recommendation 18:** The Bureau of Information Resource Management should include information security activities performed by the Office of Information Assurance in its budget submission to the Department of State. (Action: IRM)

### Contract Management

IRM/IA lacks adequate management controls and procedures for its contract management. Deficiencies exist in oversight, file maintenance, and the assignment and performance of contracting officer's representative (COR) and government technical monitor responsibilities.

IRM/IA manages five procurement vehicles with a value of more than \$79 million. IRM/IA management is examining four of the procurement vehicles—one contract, two task orders, and a blanket purchase agreement—with a total value of \$19 million and plans to end each at their respective option year. The fifth procurement vehicle—the IRM Vanguard 2.2.1 contract—is in the second of 9 option years. The IRM/IA share of the Vanguard 2.2.1 contract is approximately \$19 million through the current option year, with a total estimated value of \$60 million if all option years are exercised. The CISO plans to execute new contracts to provide office administration and data management coverage and to find an alternative means of providing C&A services currently provided through the Vanguard 2.2.1 contract—the portion of the overall IRM Vanguard contract reviewing the Department’s network and risk management.

### ***Management Oversight***

IRM/IA staff is not overseeing contracts effectively. Responsibilities of the COR and government technical monitor are assigned to individuals without the technical expertise to review the work being performed. Documentation is incomplete and lacks budget documents, labeling, or evidence of reconciliation of supporting documents.

IRM/IA has had two individuals—the Policy, Liaison, and Reporting Division chief and one staff member—managing all of its procurement vehicles. After the departure of the division chief at the beginning of this inspection, all remaining responsibilities were transferred to the staff member. This individual is responsible for tracking funds, maintaining accounting records, approving invoices, and authorizing payments and is doing so without having daily interaction with the contractors or their work and with inadequate separation of duties. While necessary COR training was taken by both individuals, no verification that continuous education and training was taken by the division chief to maintain his certification was done. The former division chief did not maintain documentation, resulting in the staff member assuming the responsibilities with little understanding of past actions. There was no information detailing deliverables, payments, balance of funds remaining, or delegations of authority. As a result, IRM/IA did not experience a smooth transition of contract responsibilities but spent a considerable amount of time locating required information during the OIG inspection.

Contract documentation showed numerous instances of incomplete files, including some without any required documents, labeling, or reconciliation. For example, one contract with a ceiling of \$2 million had inconsistencies in the deliverables and review process for payment. The contractor submits deliverables electronically to the CISO and COR, while providing hard-copy deliverables to another individual in the office for uploading to the office’s SharePoint site. The files are not readily identifiable or organized, so it is difficult to match the deliverables to the payments received. In fact, the contractor emailed the CISO and COR requesting payment for services with no deliverables attached for verification of services received. Further, the contractor provides invoices with charges for other direct costs such as travel and related expenses; however, clearer explanations of expenses are needed to provide management with clarification as to what the expenses relate.

Payments are also being made without sufficient management oversight. An invoice showed IRM/IA overpaid a contractor and, in one instance, erroneously paid for a deliverable in advance of the date it was delivered. IRM/IA principals could not locate deliverables to support payments and none of the personnel in IRM/IA were reviewing payments on a regular basis.

IRM/IA does not maintain a single repository detailing all of its respective contracts. Management could not provide the OIG team with details on contract scope, modifications, award dates, required deliverables, and invoice payment information. On one contract, the COR was not aware whether funds were available and had obligated the contract over its ceiling. Another example of mismanagement involves IRM/IA management approving invoices without authorization from the government technical monitor, and management was unable to explain years of contract inactivity on a particular task order. As a result, the Office of the Procurement Executive in the Bureau of Administration is requesting IRM/IA to deobligate \$2 million of the \$2.5 million task order if the task order is not completed by the end of FY 2013—putting the office at risk of losing \$2 million that could be used toward other office efforts.

Management is unable to verify the accuracy of reported costs. The invoices for another task order listed the number of hours worked by labor category, while the associated timesheets listed the individuals by names. Neither document links the individuals to the labor category and hours worked. The scope of the work has decreased significantly over the years and management verifies the hours of the few remaining contractors through personal interactions. The task order will terminate at the end of FY 2013 and IRM/IA is planning to execute another contract to replace it. Prior to doing so, IRM/IA should compile a breakdown of work and individuals assigned to this task order to verify cost accuracy. IRM/IA was counseled on the need to have complete documentation to verify labor hours for cost accuracy.

***Informal Recommendation 2:*** The Bureau of Information Resource Management should verify the individuals assigned and the hours worked on the time and materials procurement vehicle.

IRM/IA management is aware of the internal control weakness caused by having one individual handle all contract responsibilities with little ability to oversee the work being performed. The CISO plans to assign contract management responsibilities to other IRM/IA staff members to provide adequate oversight and separation of duties. However, no corrective actions were taken during the course of the inspection.

**Recommendation 19:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should assign the responsibilities of the contracting officer's representative and government technical monitor for the Office of Information Assurance contracts to individuals with involvement in the work performed by the contractors. (Action: IRM, in coordination with A)

**Recommendation 20:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should require the assigned contracting officer's representative and government technical monitor to maintain complete contract files. (Action: IRM, in coordination with A)

**Recommendation 21:** The Bureau of Information Resource Management should implement an internal tracking mechanism for the management of Office of Information Assurance contracts. (Action: IRM)

***Central Repository***

Contract documents are kept in several locations by IRM/IA staff, including in personal email files, an electronic library site, on the shared drive, or in hard copies. Complete contract files were not provided and IRM/IA was unable to locate missing documents, resulting in staff providing piecemeal documentation for OIG review. IRM/IA is in the process of scanning and uploading older files to its SharePoint site, but the process is illogical and unorganized. There are inconsistent naming conventions, no identification of the files or their contents, and no grouping of documents pertaining to specific contracts.

**Recommendation 22:** The Bureau of Information Resource Management should establish a central repository for Office of Information Assurance contract documentation. (Action: IRM)

***Contractors' Access to Shared Folders***

Contractors have inappropriate access to contract files. For example, third party contractors had access to folders that were unrelated to their assigned responsibilities. These folders contained government controlled information, including budget documents, contract bidding documents, and other proprietary information. Without proper procedures, the ISSO is unable to control personnel access rights, resulting in IRM/IA having the risk of sensitive materials being viewed by unapproved personnel and contractors potentially having an unfair advantage in contract procurement matters.

**Recommendation 23:** The Bureau of Information Resource Management should require the Office of Information Assurance to implement procedures for granting system access to its personnel. (Action: IRM)

**Recommendation 24:** The Bureau of Information Resource Management should require the Office of Information Assurance to review the system access rights of its contract staff for viewing folders on the shared network and restrict permissions as appropriate. (Action: IRM)

***Inherently Governmental Functions***

Several IRM/IA contractors are performing inherently governmental functions. These functions include drafting responses to OIG audit reports and reviewing and clearing pending legislation on behalf of IRM/IA. In addition, contractors appear to be performing services and actions that may be inherently governmental and require closer monitoring. One contractor could view emails sent to the CISO, allowing the individual access to potentially confidential or sensitive materials. Contractors were also responding to Department officials on policy-related issues. Further, contractors were handling personnel matters including interacting with the Bureau of Human Resources on position description revisions and vacancy announcements and developing the proposed IRM/IA reorganization package. IRM/IA management must take the necessary steps to remove contractors from performing such actions.

**Recommendation 25:** The Bureau of Information Resource Management should review the work being performed by contractors in the Office of Information Assurance and reassign the inherently governmental functions to a government direct-hire employee. (Action: IRM)

### *Vanguard 2.2.1 Contract Management*

The IRM/IA-related scope of the Vanguard 2.2.1 contract has not been managed appropriately. Specifically, the CISO changed the scope of the C&A work twice throughout the process without consideration of the ramifications on the workload. Most importantly, there is a lack of communication among responsible parties. These combined factors have resulted in the Department having expired authorizations to operate 52 of its 309 systems. The Vanguard 2.2.1 contract is a 10-year vehicle with a total estimated value of \$2.5 billion; the current IRM/IA portion of the contract is approximately \$19 million through current option year 2 and projected to reach a total estimated value of \$60 million if all options are exercised.

The C&A contract scope went through a major change after the contract award process. Originally, when the Department released a request for procurement, the statement of work noted that the Department did traditional C&A activities and was planning to move towards continuous monitoring for its systems. The request stated that traditional C&A activities would cease when the changeover was made to continuous monitoring, thus requiring minimal staff support. However, after the contract was awarded, the previous CISO departed and the Chief Information Officer at that time decided to resume traditional C&A activities and to also include C&A work for OpenNet and ClassNet. The renewed C&A activities increased the scope of the contract and resulted in an increase in work and expenses for the contract company, which was not fully prepared for the additional workload now required by the Department.

IRM management then eliminated continuous monitoring from the scope of the contract, which resulted in cost savings of about \$13 million over the life of the contract. Because the Department could not do OpenNet and ClassNet assessments under continuous monitoring, it needed to include a \$1.8 million time and material project to perform the traditional C&A assessment. IRM spent the additional funds without monitoring the work of the contractor.

Lack of communication among responsible parties is a major issue. IRM/IA is experiencing problems with the work performed by the C&A contractors. Specifically, the contractors are unable to keep up with the workload, resulting in many systems having expired authorizations to operate. The Vanguard COR was unaware of these issues since IRM/IA has not conveyed any details to the individual or the program office for the COR. In fact, weekly assessment reports from the IRM/IA government technical monitor contained no description of problems with the workload and contractor performance. The Vanguard COR became aware of the seriousness of the scope of the contract not being met only after the OIG team conveyed the issues. The CISO recently began pursuing an alternative means of performing the C&A work during the OIG inspection—a matter which, once again, the Vanguard COR has not been made aware.

According to IRM/IA management, they are working with the Bureau of Administration to complete a Request for Information to gather data concerning the funding and staffing requirements of completing C&A reviews for the Department's information systems. Once the information is received, a determination will be made by the CISO regarding future C&A work under the Vanguard 2.2.1 contract.

**Recommendation 26:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should determine how future certification and accreditation work will be performed under the Vanguard 2.2.1 contract. (Action: IRM, in coordination with A)

### **Inventory Management**

An inventory check identified 57 computers, 6 printers, and 2 monitors as excess inventory for IRM/IA. According to 14 FAM 427.1, property that is no longer needed by an office should not be allowed to accumulate in office spaces. Transferring the excess equipment will streamline IRM/IA property records and reduce the potential threat of loss or mishandling.

**Recommendation 27:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should dispose of excess information technology equipment for the Office of Information Assurance. (Action: IRM, in coordination with A)

### **Training**

IRM/IA has not developed an officewide training curriculum for its employees nor does each staff member have an individual development plan. Training records from the Bureau of Administration, which is the executive office of IRM/IA, show that management has not taken required management and leadership training. Many employees reported that they did not have individual development plans. In accordance with 13 FAM 022.3 and 3 FAH-1 H-2821.3 a.(3), directors and managers should ensure that training needs are identified and outlined in an individual development plan. Because the focus of IRM/IA is information security, staff and management need to have the relevant knowledge and skills and remain abreast of new technology by receiving regular training.

**Recommendation 28:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should implement a training curriculum for the Office of Information Assurance that outlines required and recommended training for all staff levels and functions. (Action: IRM, in coordination with A)

**Recommendation 29:** The Bureau of Information Resource Management should require an individual development plan for each Office of Information Assurance employee. (Action: IRM)

### **Equal Employment Opportunity**

IRM/IA would benefit from having an in-house counselor to assist with Equal Employment Opportunity concerns. During the course of this inspection, IRM/IA was handling one formal complaint as well as two employee relations cases. Currently, IRM/IA employees report Equal Employment Opportunity matters directly to the Office of Civil Rights, which provides guidance to employees. While having an internal counselor is not required by Department regulations, a counselor would provide an informed view of the compliance of IRM/IA with Equal Employment Opportunity principles and assist staff with facilitating their concerns.

***Informal Recommendation 3:*** The Bureau of Information Resource Management should designate an Equal Employment Opportunity counselor to assist staff with guidance and resolving issues.

### **Performance Plans and Employee Appraisals**

Many employees have not received their 2012 employee performance appraisals or received their performance plans for 2013. According to documentation received from the Bureau of Human Resources dashboard, 2012 employee performance appraisals and 2013 employee performance plans have been completed for the CISO and the IRM/IA division chiefs; however, each division chief has not completed their respective staff members' appraisals or performance plans. Prompt attention by the CISO in directing his division chiefs to complete these mandatory performance documents is necessary.

IRM/IA management indicated to the OIG team that 2013 performance plans will be completed by June 2013. IRM/IA management stated that an agreement between the union and the Bureau of Human Resources, Labor Relations Office, determined that those individuals who did not receive 2012 performance plans will not be given performance appraisals for that year.

**Recommendation 30:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should complete 2012 employee performance appraisals and 2013 employee performance plans for the Office of Information Assurance staff. (Action: IRM, in coordination with A)

### **Orientation for Incoming Personnel**

IRM/IA does not have an orientation packet for incoming personnel. Personnel either became familiar with the organization and position by asking questions or having an unofficial mentor. A comprehensive orientation packet would provide the staff with a common understanding of the functions of the office and its role in the Department.

***Informal Recommendation 4:*** The Bureau of Information Resource Management should direct the Office of Information Assurance to develop an information packet for incoming personnel.

### **Physical Security**

#### ***Principal Unit Security Officer***

IRM/IA does not have a primary principal unit security officer as required by 12 FAM 563.1. The former officer departed IRM/IA and the assigned alternate is performing the function on a collateral basis along with his property officer responsibilities. Per FAM regulations, the head of each major functional area must designate a principal unit security officer to assist in carrying out the area's security responsibilities.

**Recommendation 31:** The Bureau of Information Resource Management should appoint a principal unit security officer for the Office of Information Assurance. (Action: IRM)

*Closing Hours Security Check*

IRM/IA does not have an acceptable process for performing security checks at closing hours. Security container checklists are not used daily as part of securing safes. Further, staff does not have shared responsibility to perform a walk around at closing hours to ensure the work space is secure. In accordance with 12 FAM 534.2, supervisors should institute a system of designating employees to conduct closing hours security checks on a weekly basis. By doing so, IRM/IA can help ensure that classified material is properly stored and secured.

**Recommendation 32:** The Bureau of Information Resource Management should direct the Office of Information Assurance to implement a closing hours security check. (Action: IRM)

## List of Recommendations

**Recommendation 1:** The Bureau of Human Resources should direct the Office of Resource Management and Organizational Analysis to perform an organization assessment of the Bureau of Information Resource Management, Office of Information Assurance, including a workforce and workload balance analysis and a review of similar functions that are being performed by other offices in the Department of State. (Action: DGHR)

**Recommendation 2:** The Bureau of Information Resource Management should develop a written mission statement for the Office of Information Assurance that includes short-term and long-term priorities and goals for the office and each division. (Action: IRM)

**Recommendation 3:** The Bureau of Information Resource Management should revise its Department of State Information Technology Strategic Plan to include the Office of Information Assurance activities. (Action: IRM)

**Recommendation 4:** The Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, should direct the Office of Information Assurance to update Volume 5 of the *Foreign Affairs Manual* and *Foreign Affairs Handbook*. (Action: IRM, in coordination with DS)

**Recommendation 5:** The Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, should implement a clearance process for revisions and updates to the *Foreign Affairs Manual* and *Foreign Affairs Handbook* that includes the review and approval of both bureaus. (Action: IRM, in coordination with DS)

**Recommendation 6:** The Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, should establish *Foreign Affairs Manual* and *Foreign Affairs Handbook* policies on information technology security exceptions, including descriptions of types of exceptions and procedures for requesting waivers. (Action: IRM, in coordination with DS)

**Recommendation 7:** The Bureau of Information Resource Management should require the Office of Information Assurance to participate regularly in Departmentwide information technology working group meetings and share learned information from such meetings with its staff. (Action: IRM)

**Recommendation 8:** The Office of the Under Secretary for Management, in coordination with the Bureaus of Diplomatic Security and Information Resource Management, should assign responsibility of the information systems security officer program to a single bureau. (Action M/PRI, in coordination with DS and IRM)

**Recommendation 9:** The Bureau of Information Resource Management should survey system owners on issues they are encountering with certification and accreditation tools and take necessary corrective steps to improve the certification and accreditation tools, guidance, templates, and procedures. (Action: IRM)

**~~SENSITIVE BUT UNCLASSIFIED~~**

**Recommendation 10:** The Bureau of Information Resource Management should develop a control process for changes to certification and accreditation templates and guidance that includes advance notice to system owners of pending changes. (Action: IRM)

**Recommendation 11:** The Bureau of Information Resource Management should identify the common security controls for its Department of State systems. (Action: IRM)

**Recommendation 12:** The Bureau of Information Resource Management should document the necessary review steps to be performed by each certification and accreditation assessor. (Action: IRM)

**Recommendation 13:** The Bureau of Information Resource Management should develop an action plan to address all Department of State systems with expired authorizations to operate. (Action: IRM)

**Recommendation 14:** The Bureau of Information Resource Management should assign an individual to review and reconcile certification and accreditation reimbursements between the Corporate Budget Allocation Tracking System and the Bureau of Information Resource Management's internal funding spreadsheet. (Action: IRM)

**Recommendation 15:** The Bureau of Information Resource Management should provide system owners with close-out reports for verification of associated certification and accreditation costs. (Action: IRM)

**Recommendation 16:** The Bureau of Information Resource Management should develop project management documentation for iPost. (Action: IRM)

**Recommendation 17:** The Bureau of Information Resource Management should assign a content manager and define a content management process for managing the content on its Office of Information Assurance Web site and shared network. (Action: IRM)

**Recommendation 18:** The Bureau of Information Resource Management should include information security activities performed by the Office of Information Assurance in its budget submission to the Department of State. (Action: IRM)

**Recommendation 19:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should assign the responsibilities of the contracting officer's representative and government technical monitor for the Office of Information Assurance contracts to individuals with involvement in the work performed by the contractors. (Action: IRM, in coordination with A)

**Recommendation 20:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should require the assigned contracting officer's representative and government technical monitor to maintain complete contract files. (Action: IRM, in coordination with A)

**Recommendation 21:** The Bureau of Information Resource Management should implement an internal tracking mechanism for the management of Office of Information Assurance contracts. (Action: IRM)

**~~SENSITIVE BUT UNCLASSIFIED~~**

**Recommendation 22:** The Bureau of Information Resource Management should establish a central repository for Office of Information Assurance contract documentation. (Action: IRM)

**Recommendation 23:** The Bureau of Information Resource Management should require the Office of Information Assurance to implement procedures for granting system access to its personnel. (Action: IRM)

**Recommendation 24:** The Bureau of Information Resource Management should require the Office of Information Assurance to review the system access rights of its contract staff for viewing folders on the shared network and restrict permissions as appropriate. (Action: IRM)

**Recommendation 25:** The Bureau of Information Resource Management should review the work being performed by contractors in the Office of Information Assurance and reassign the inherently governmental functions to a government direct-hire employee. (Action: IRM)

**Recommendation 26:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should determine how future certification and accreditation work will be performed under the Vanguard 2.2.1 contract. (Action: IRM, in coordination with A)

**Recommendation 27:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should dispose of excess information technology equipment for the Office of Information Assurance. (Action: IRM, in coordination with A)

**Recommendation 28:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should implement a training curriculum for the Office of Information Assurance that outlines required and recommended training for all staff levels and functions. (Action: IRM, in coordination with A)

**Recommendation 29:** The Bureau of Information Resource Management should require an individual development plan for each Office of Information Assurance employee. (Action: IRM)

**Recommendation 30:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should complete 2012 employee performance appraisals and 2013 employee performance plans for the Office of Information Assurance staff. (Action: IRM, in coordination with A)

**Recommendation 31:** The Bureau of Information Resource Management should appoint a principal unit security officer for the Office of Information Assurance. (Action: IRM)

**Recommendation 32:** The Bureau of Information Resource Management should direct the Office of Information Assurance to implement a closing hours security check. (Action: IRM)

## List of Informal Recommendations

Informal recommendations cover operational matters not requiring action by organizations outside the inspected unit and/or the parent regional bureau. Informal recommendations will not be subject to the OIG compliance process. However, any subsequent OIG inspection or on-site compliance review will assess the mission's progress in implementing the informal recommendations.

***Informal Recommendation 1:*** The Bureau of Information Resource Management should require the Office of Information Assurance to develop an office strategic plan that aligns with its mission and goals and with the Department of State's Information Technology Strategic Plan.

***Informal Recommendation 2:*** The Bureau of Information Resource Management should verify the individuals assigned and the hours worked on the time and materials procurement vehicle.

***Informal Recommendation 3:*** The Bureau of Information Resource Management should designate an Equal Employment Opportunity counselor to assist staff with guidance and resolving issues.

***Informal Recommendation 4:*** The Bureau of Information Resource Management should direct the Office of Information Assurance to develop an information packet for incoming personnel.

## **Principal Officials**

	<b>Name</b>	<b>Arrival Date</b>
CISO/Director	William Lay	09/12
Deputy Director	Gary Galloway	11/12
System Authorization Division	Charles —Rady” Johnson	01/13
Global Oversight Division	Mark Mitchell	08/10
Policy, Liaison, and Reporting Division	Ron Austin*	04/12

\*Departed 02/13.

## Abbreviations

C&A	Certification and accreditation
CBATS	Corporate Budget Allocation Tracking System
CISO	Chief information security officer
COR	Contracting officer's representative
Department	U.S. Department of State
DS	Bureau of Diplomatic Security
FAH	<i>Foreign Affairs Handbook</i>
FAM	<i>Foreign Affairs Manual</i>
FISMA	Federal Information Security Management Act of 2002
IRM/IA	Bureau of Information Resource Management, Office of Information Assurance
ISSO	Information systems security officer
IT	Information technology
OIG	Office of Inspector General
QDDR	Quadrennial Diplomacy and Development Review



**FRAUD, WASTE, ABUSE,  
OR MISMANAGEMENT  
OF FEDERAL PROGRAMS  
HURTS EVERYONE.**

CONTACT THE  
OFFICE OF INSPECTOR GENERAL  
HOTLINE  
TO REPORT ILLEGAL  
OR WASTEFUL ACTIVITIES:

202-647-3320

800-409-9926

[oighotline@state.gov](mailto:oighotline@state.gov)

[oig.state.gov](http://oig.state.gov)

Office of Inspector General  
U.S. Department of State  
P.O. Box 9778  
Arlington, VA 22219