Office of Inspector General

United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General

Office of Inspections

Inspection of the Bureau of Information Resource Management, Systems and Integration Office

Report Number ISP-I-12-30, June 2012

~~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 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 instance 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.

Harold W. Geisel
Deputy Inspector General

Table of Contents

Key Judgments	1
Context	2
Executive Direction	4
Mission and Goals	4
Leadership	4
Communication	5
Program Implementation	7
Contract Management	7
Systems Development Life Cycle	9
Program Management Functions	10
Development Network	11
Business Engagement Center Division	13
Planning, Acquisition, and Budget Branch	13
Information Management Support Branch	15
Enterprise Server Operations Center Customer Management Branch	16
Enterprise Server Operations Center Divisions	18
Operations and Maintenance Division	18
Design and Build Division	20
Customer and Executive Information System	21
Cloud Computing	21
Collaboration and Compensation Services Division	24
Enterprise Collaboration Services Branch	24
Compensation Applications Branch	28
Enterprise Programming and Integration Division	30
Data Management Branch	30
Integrated Projects Branch	30
Application Development Branch	31
Program Management Office	31
List of Recommendations	33
List of Informal Recommendations	36
Principal Officials	37
Abbreviations	38

Key Judgments

- The Systems and Integration Office (SIO) has a knowledgeable, hardworking, and engaged management team that, for the most part, effectively dispatches its duties, which involve a wide range of new and old technologies, centralized and decentralized models of network management, budgetary items it can and cannot control, as well as colocated and dispersed physical locations.

- SIO senior leadership has made a concerted effort to promulgate a cohesive mission statement and goals to direct the activities of the office.

- SIO's implementation of cloud computing does not fulfill the essential characteristics of cloud computing as defined by the National Institute of Standards and Technology (NIST).

- SIO lacks adequate controls and procedures to monitor its multiyear contracts totaling more than $182 million.

- The use of SharePoint sites has grown significantly beyond the intended scope of this application, with many employing SharePoint to conduct daily business as well as support key political and military events.

- SIO management has not enforced use of the systems development lifecycle (SDLC) process and methodology in all its relevant divisions and branches.

- Management needs to define clearly the role and organizational placement of the Program Management office and function and to standardize the use of terminology referring to office activities.

- Communication in all areas of SIO's business needs improvement.

- SIO's internal inventory process for managing and tracking is poorly defined and documented.

- SIO management has not begun working on a formal plan for the Compensation Application branch regarding the transition of the payroll support function to the Bureau of Resource Management.

The inspection took place in Washington, DC, between February 6 and March 16, 2012.
(b) (6) [redacted]

Context

SIO is one of six functional areas of the Operations directorate in the Bureau of Information Resource Management (IRM). SIO traces its origins back to the Department of State's (Department) establishment of the Automated Data Processing Office in 1959. After several reorganizations, that office evolved into SIO, which today provides application development, software integration, and enterprise server management services. The full scope of SIO's functions often overlaps with other areas of IRM and the Department, but it formally defines its mission as to "empower diplomacy with robust cloud computing, collaborative services, and integrated software solutions."

SIO develops, deploys, and supports numerous applications at more than 200 posts and 28 bureaus. It has three data centers that provide enterprise server management for domestic bureaus, including support of the mainframe system that controls the Department's payroll. SIO is known in the Department for some of its more widely used products and services such as Post Administrative Software Suite, eCountry Clearance, Enterprise Server Operations Center, and Microsoft Office SharePoint Server 2007.

SIO has five divisions supporting its mission. The Enterprise Server Operations Center (ESOC) Design and Build (D&B) division supports the standup of the enterprise-wide data centers and the Federal Data Center Consolidation Initiative. The ESOC Operations and Maintenance (O&M) division supports the operation of the data centers. The Collaboration and Compensation Services (CCS) division maintains the Department's legacy payroll systems and provides enterprise-wide SharePoint technical support. The Enterprise Programming and Integration (EPI) division is responsible for several enterprise-wide software solutions, the enterprise service bus, and data management initiatives. The Business Engagement Center (BEC) division provides contract, budget, and administrative support to SIO.

SIO has developed five strategic goals for FYs 2012 and 2013 to link to the Department's Information Technology (IT) Strategic Plan. The first goal is the design and build of the ESOC West data center, including activities to automate and modernize backups and to support cloud computing, virtualization, and the Federal Data Center Consolidation Initiative. The second includes planning for upgrades and capacity growth, as well as customer service and performance measurement support. The third focuses on further development of collaboration services such as SharePoint, as well as sunsetting legacy mainframe applications. The fourth includes ambitious plans to implement Web services hosted on a centralized enterprise service bus, standardize metadata, and enhance enterprise applications. The fifth goal includes implementing financial management and inventory control, as well as monitoring service level agreements (SLA) with bureaus that have moved forward with data center consolidation with SIO.

The last goal will prove increasingly important as Department implementation of its recently entered Vanguard contract looms over SIO and IRM. The Vanguard effort is a Department initiative to consolidate all IRM contract activities under one performance-based contract. As such, it should compel a paradigm shift in the way IRM does business, as Department IT managers will have to adapt to a model of managing user expectations and

evaluating contractor performance against the contract terms versus managing resources and affecting outcomes directly. There will be attendant consequences on most aspects of SIO operations and organizational structure as SLAs are crafted to mold operations to the lines of business outlined in the contract.

According to IRM, SIO has 77 full-time employees with 14 vacant positions. There are also 205 contractors from 14 different contract companies supporting SIO operations. The total value for the life of these contracts, which are paid under the umbrella of the HITTS contract, is approximately $182 million. In FY 2011, SIO's annual operating budget was approximately $72.2 million. SIO's FY 2013 budget request was for more than $82 million.

Executive Direction

Mission and Goals

SIO senior leadership has made a concerted effort to develop and promulgate a cohesive mission statement to direct the activities of the office. Motivated by recent Office of Inspector General (OIG) reports highlighting the lack of such mission statements in other offices, SIO created a new mission statement that focuses on cloud computing, collaborative services, and integrated software solutions and posted it prominently around the office just prior to the OIG inspection. The statement is broad, technology neutral, and links SIO's work to the Department's business of diplomacy. However, the OIG team questions whether the statement is so broad that many employees may not understand how to contribute toward achieving it; for example, do system administrators or software developers working on SharePoint understand they are supporting the "platform as a service" portion of NIST's cloud computing model? Interestingly, the first line on the "About Us" page of SIO's intranet site describes the office as "the Department's primary source for application development, software integration, and enterprise server management." The OIG team found that language to be more succinct in describing the office's role in the Department. Nevertheless, time will tell whether the new mission statement will prove meaningful to SIO employees and help guide their efforts.

SIO also developed a document detailing its strategic goals and objectives; however, this information appears to bypass the SIO mission statement and be more aligned with the Department's IT Strategic Plan. The document does have significant detail and demonstrates a commitment to larger Department goals. This commitment will be tested soon and for the coming years as IRM proceeds with the consolidation of all its contract activities under the performance-based Vanguard contract. Additionally, the Department's retooling of the strategic planning and resource management process, along with an expected update of IRM's IT Strategic Plan, provides an opportunity to revise SIO's new mission statement to better reflect the office's role. It will be important for SIO management to keep its focus on a potentially moving target and to treat its mission statement as part of a planning and implementing process requiring regular reviews, rather than as a completed checkmark.

> ***Informal Recommendation 1:*** The Bureau of Information Resource Management should conduct periodic reviews of the Systems and Integration Office's mission and goals to measure its progress in meeting the Department of State's information technology strategic goals and make revisions as needed.

Leadership

The OIG team observed a knowledgeable, hardworking, and engaged management team that, for the most part, effectively dispatches its duties, which involve a wide range of disparate responsibilities that require working with both new and old technologies, centralized and decentralized models of network management, budgetary items it can and cannot control, as well as colocated and dispersed physical locations. The SIO director joined the office in January 2007. IRM senior leadership universally lauds her abilities and achievements, and division and branch chiefs within SIO had positive comments about her leadership qualities. Other feedback

included generally favorable scores on OIG's inspection survey, with the interesting anomaly that full-time employee survey scores were slightly lower than contractor scores across the board. Those that reported having the most regular contact with the Director provided high praise, while those at lower levels with less frequent or no interaction with her had some complaints related to office communication and dissemination of management priorities. There were similar comments regarding the leadership qualities of division and branch chiefs, with some frustration about inconsistent organizational communication.

Within SIO, the OIG team encountered various accounts of leadership at the division and branch levels. Some are satisfied with how their group conducts its business; however, others complain about how the entity translates broader office goals into prioritized tasks. Some groups have been setting the scope of their work too broad, causing them to lose focus. Some complain that priorities change daily based on who is complaining the loudest. Priorities tend to be fluid, with constantly changing deliverable dates. Others note a lack of risk planning when translating goals into tasks. Additionally, the common use of matrix resources appears to have led to conflicting priorities and timelines for project deliverables. These issues generally relate to communication of management priorities and implementation of organizational processes to achieve them.

A fairly common complaint among survey respondents and those interviewed during the inspection was that SIO does not have sufficient representation with senior IRM leadership. Some thought that key SIO products are often ignored or not funded, despite holding high significance with respect to the Department's IT Strategic Plan. Some criticized the director for not sufficiently promoting SIO's products with IRM senior management. Likewise, integration within and across IRM has been spotty and problematic, occasionally hampering SIO's productivity when it must rely on other IRM organizational elements. Continued management engagement with other IRM directorates and offices will be necessary to achieve effective collaboration on projects.

Communication

Communication in all areas of SIO's business needs improvement, with the possible exception of that with other agencies. The OIG team encountered myriad complaints of ineffective communication within SIO, within IRM as a whole, and with other bureaus in the Department. (b) (5) [redacted] SIO management has made earnest efforts to improve communication, including various types of all-hands meetings, SharePoint sites, team-building exercises, and newsletters, but has yet to find the right balance. The challenges are numerous, including highly disparate employee functions and backgrounds, significant turnover in contract employees, and dispersed work locations. The move of some staff to State Annex 9 has helped in some respects but has also led to complaints of too much communication, with offices having to sift through duplicate copies of the same information. Poor cross-team and interbureau communication is also a problem, with managers in other bureaus eschewing the proper channels and escalation procedures and instead communicating directly with a manager in SIO. Although this strategy works well for the individual, it circumvents the processes in place and impedes communication as a whole. The technology meant to enhance communication has also sometimes been the source of frustration, with messages being sent out in a scattershot manner and involving too many recipients to be

productive. Meanwhile, many complained that most of the larger staff, all-hands, and other meetings on the already busy SIO schedule seem to rehash old information and thus are a waste of time. Others are weary of the leadership's attempts at team-building exercises. The SIO director has planned to resume periodic newsletters as a means of communicating better with her staff.

Program Implementation

Contract Management

SIO currently has nine separate task orders under six contracts, with a total value of more than $182 million. Each contract is for a performance period ranging from 3 to 5 years. SIO functions will be consolidated as part of the 2.3.x series under the Vanguard effort, which is a Department initiative to consolidate all IRM contract activities under the umbrella of one performance-based contract with multiple task orders. SIO's existing task orders—SharePoint Operations and Maintenance, ESOC Operations, IRM Applications Operations and Maintenance, Data Management, and Integrated Project—will be part of the 2.3.x series. The compensation task order, which supports the responsibilities for the legacy payroll function that will be transferred to the Bureau of Resource Management, is not part of this effort.

SIO management has spent considerable time planning for the transition to the Vanguard contract and has established a Vanguard Project Team to assist with this effort. The Vanguard Project Team is led by the EPI division chief, with management representation from the other SIO divisions, the other IRM elements, and the executive office of the Bureau of Administration. The project team meets weekly and discusses progress made to date. Assigned individuals are reviewing the scope of services of existing contracts and developing performance metrics for evaluating the work performed. SIO is benefitting from lessons learned from the Vanguard 2.2.1 implementation and seems to be taking the needed time to plan. The OIG team encourages SIO to continue with its planning efforts for the Vanguard 2.3.x series and to be mindful of the importance of continuous communication with affected parties to ensure a smooth transition.

Central Repository

SIO lacks adequate procedures and controls to monitor contracts and the work performed by contractors. Contract documentation is located in multiple places, including personal emails, several electronic library sites, and in hard copy. SIO maintains at least three electronic library sites but does not have a mechanism for grouping the documentation together in a logical, systematic way or for linking documents to the other library sites. Upon review of library files, the OIG team found duplicate and incomplete documentation, inconsistent naming conventions, and no verification that the contracting officer's representatives (COR) and government technical monitors (GTM) have accessed and reviewed the files.

The recently created SIO Financial Private Library, which is the repository of contracts, agreements, training certifications, and delegations of authority for the CORs and GTMs, is also not organized so that the user can easily locate and/or review documents. The OIG team found no complete contract files containing contract deliverables such as monthly reports, meeting minutes, or correspondence between the COR/GTM and contractor in an accessible location. Further, although the financial library used internally by BEC management contains contractor invoice files, it does not show evidence of payment approvals. Based on the OIG team's suggestion, BEC staff recently started uploading files such as invoices and emails to the financial library. However, these invoices are still being filed in the same manner as the earlier invoices, making it difficult to identify the invoice dates without opening each document.

Recommendation 1: The Bureau of Information Resource Management should establish a central repository for the management of Systems and Integration Office contracts so that all relevant documentation for each contract, such as statements of work, amendments, and invoices, are in one central location. (Action: IRM)

SIO management also does not have a centralized process for determining the status of obligations or funds for each contract. SIO provided the OIG team with a spreadsheet, dated January 27, 2012, listing the contract ceiling limits and total amount spent for each contract. The OIG team found several factual errors, including incorrectly identified contract option years and expiration dates. The team also found that the total amount spent on the contracts had not been updated on the spreadsheets from January 13 to March 14. The process for invoicing involves multiple parties and steps, making the need for better management of contract funding and obligations even more pressing. Currently, division chiefs or GTMs verify contractor labor hours against the time and attendance information entered in either the Project Tracking System or Customer and Executive Information System (CEIS). Then the information is sent via email to BEC division staff members who compare the contractor invoices against the contract, verify fund availability, and complete the invoice approval form sent to Global Financial Services Charleston for payment. SIO estimates that it pays approximately 400 invoices per year. It is in SIO's interest to continually track funds to help ensure accountability and meet priorities and goals.

Recommendation 2: The Bureau of Information Resource Management should prepare a funding document that details the authorized, spent, and remaining funds for each Systems and Integration Office contract and implement procedures to verify and update this information regularly. (Action: IRM)

Contracting Officer's Representative and Government Technical Monitor Assignments

The process for assigning COR and GTM responsibilities for SIO contracts needs improvement. Specifically, individuals assigned with such responsibilities appear to have little or no daily interaction or involvement with the corresponding contractor and scope of work. For example, one assigned COR is also the GTM for the same contract, which has multiple task orders. The individual commented on the inability to verify the labor hours and work for the contractors because the work being performed does not directly affect his specific division but rather the rest of SIO.

COR and GTM responsibilities in SIO are either assigned to division chiefs, SIO staff members, or a representative from the Bureau of Administration. SIO-assigned individuals perform their duties with varying degrees of diligence. Some of the CORs and GTMs have constant interaction with their contractor staff, either via emails or face-to-face meetings, and maintain supporting documentation to evaluate contractor performance. Other GTMs and CORs within SIO, however, could neither articulate their responsibilities for contract oversight nor produce documentation showing their continuous review of performance.

SIO-provided documentation shows all CORs and GTMs have completed the required training, but only half have received the mandatory Federal Acquisition Certification for CORs and GTMs that qualifies them for such appointments, as detailed in Procurement Information

Bulletin No. 2010-20. As of July 2010, the Bureau of Administration requires all CORs and GTMs who hold delegation letters on active contracts to be certified no later than 6 months from the date of assignment.

Improper assignment of CORs and GTMs, as well as their incomplete training, affects SIO management's ability to manage and oversee the work of its contractors. The responsibility for a COR or GTM is not always assigned to an individual who can provide the needed frequent interaction and oversight of the contractor's work and scope of services. If not corrected, this issue could lead to overpayment of contractors or failure to meet project goals. Given the more than 200 individual contractor employees supporting SIO operations, the OIG team encourages SIO management to take immediate action.

Recommendation 3: The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should assign the responsibilities of contracting officer's representatives and government technical monitors for Systems and Integration Office contracts to individuals who have the technical expertise to evaluate the scope of work performed by the contractors. (Action: IRM, in coordination with A)

Recommendation 4: The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should implement a policy requiring all assigned contracting officer's representatives and government technical monitors for Systems and Integration Office contracts to apply for Federal Acquisition Certification by completing the required training and submitting corresponding documentation to the Office of the Procurement Executive in accordance with Department of State guidelines. (Action: IRM, in coordination with A)

Contractors Managing Staff

The OIG team identified a contractor who was improperly managing full-time employees within the SIO organization by providing them with direction on assignments, project priorities, and daily management of tasks. The OIG team informed the relevant division chief, and corrective steps are being taken to address the problem. (See the Enterprise Programming and Integration Division section of this report for more details.)

Systems Development Life Cycle

Methodology

Within SIO, EPI is seen as the driving force in directing its SDLC process. In fact, the majority of SIO's systems development activities occur within EPI, which is the only division that includes systems development in its mission statement. An SDLC process defines the recommended procedure by which an organization envisions, defines, builds, deploys, operates, and maintains its systems and applications. An SDLC process is intended to establish a consistent, repeatable, and transparent process that can be tailored to a variety of project types.

With the efforts of EPI personnel, SIO documented and approved an SDLC process in November 2011. The documentation clearly defines the control gates for each phase of the process (initiation, planning design, test and deployment, and closeout), including required

management approval and documentation. EPI's documented SDLC process has been used and tailored by the other SIO divisions for their specific needs. CCS's development activities, for example, are split primarily between payroll applications and SharePoint development. The payroll application development uses structured methodologies associated with legacy programming languages, whereas SharePoint development employs project development plans based on a traditional waterfall approach—a developmental methodology whereby a project moves to the next phase only upon completion and perfection of the preceding phase. CCS has borrowed from EPI in much of that approach.

SIO is currently reviewing its SDLC process to align it more closely with the Agile methodology, which highlights requirements and solutions that evolve through collaboration between teams. With more engagement with the customer, Agile methodology promotes adaptive planning and development and delivery while encouraging rapid and flexible response to change. However, SIO has not documented the Agile methodology effectively to ensure cohesion within the existing documented process. Upon review, the OIG team found that Agile terminology is included in the document; however, it does not include control gates or details on the collaboration needed among teams and with customers. Further, the details on the Agile methodology appear to be described more as a hybrid process that includes some aspects of a waterfall methodology. When questioned, SIO management commented that a strict Agile methodology would not work across all SIO's prospective projects, hence the hybrid approach. SIO has not established the process and criteria for determining which methodology to employ for each project, resulting in a potentially indeterminate gray area of hybrid combinations. This lack of rigor hampers SIO management's ability to evaluate the completeness of documentation and the performance management review of each respective project.

Recommendation 5: The Bureau of Information Resource Management should clearly document the alternative systems development methodologies and criteria for use of each methodology in Systems and Integration Office development activities. (Action: IRM)

Project Tracking

The development of the Project Tracking System has assisted SIO in providing a platform for consistency in and enforcement of the SDLC process. The system is based on the Microsoft Project Server application and currently houses the information for several projects. The OIG team received a demo of the Project Tracking System and found it to provide the general requirements for project tracking. However, the system is not being used by all divisions and branches.

Recommendation 6: The Bureau of Information Resource Management should document which tool to use for centralized project tracking for Systems and Integration Office projects and enforce compliance among personnel. (Action: IRM)

Program Management Functions

SIO has not clearly defined the role and organizational placement of the Program Management office and function or the use of terminology referring to its activities. Currently, SIO has multiple individuals acting in a program management or process improvement capacity.

Further, terms such as "program management" and "process improvement" are used interchangeably within the office to describe the work of multiple individuals who perform similar functions.

Program management/process improvement functions are under the purview of a Program Management office within the EPI division that comprises 4 full-time employees and 14 contractors. These individuals are responsible for project management process improvement, IT security and compliance, configuration management, and architecture of EPI operations. Additionally, another individual within EPI functions as an advisor on special projects. SIO has also recently established a process improvement position reporting directly to the SIO director. The role of this individual is still being defined per discussions held with SIO management. In fact, this individual is performing functions under his previous responsibilities and has yet to reside full time in his new role. Further, the SIO director has recently informed management about possibly establishing a separate Program Management office within the BEC division.

It is unclear how the SIO director views the role of the Program Management office. The director commented that each division has good processes, and she is not certain of what, if any, are missing. Although the incumbent of the process improvement position is responsible for completing an inventory of all processes, as stated earlier, this individual has not yet assumed his new duties. The SIO director is unaware of what overlaps may be present with the other process-focused positions and entities within SIO and plans to address this issue upon completion of the inventory of processes.

The OIG team expected that SIO would have conducted an analysis of existing processes and program management functions prior to filling any positions or making any organizational changes. Without such planning, confusion about responsibilities is inevitable. Management guidance is lacking on whether SIO will spread these specific roles throughout the office or consolidate them within one division/branch, as well as on the actual role and function of the Program Management office.

Recommendation 7: The Bureau of Information Resource Management should determine the role and organizational placement of the Program Management office and function within the Systems and Integration Office and define terminology pertaining to program management activities. (Action: IRM)

Development Network

SIO is not monitoring its development network properly. The development network, DevLan, is a stand-alone network used for development activities for SIO software programs and is handled jointly by the CCS and EPI divisions. CCS administrators manage the DevLan servers, while both EPI and CCS staff provide oversight for patches and antivirus updates.

(b) (5)

[redacted]

(b) (5) [redacted]

Recommendation 8: (b) (5) [redacted]

Recommendation 9: (b) (5) [redacted]

Business Engagement Center Division

The BEC division handles most of the administrative functions for SIO. The division chief and branch chiefs communicate effectively, meeting regularly to discuss the status of current projects and share pertinent information. BEC management also participates in Department-wide meetings to represent the views of SIO, indicating that the division chief has the trust of SIO management. However, BEC needs to improve its budgeting and inventory processes, as well as contract management, which is discussed earlier in the report. Most important, BEC employees could be structured more effectively for SIO by transferring some of their responsibilities to another SIO division, providing BEC the opportunity to focus more on its core functions.

BEC consists of three branches: Planning, Acquisition, and Budget; Information Management Support; and ESOC Customer Management. A staff of 10 full-time employees and 5 contractors provide project tracking, customer service management, and inventory management services, as well as internal SIO acquisitions, budgeting, and contract management functions.

Planning, Acquisition, and Budget Branch

The Planning, Acquisition, and Budget branch is responsible for most of BEC's functions. The six-person team manages the SIO inventory, software licensing, budgeting, contract management, acquisitions, credit card purchases, and office supplies for all of SIO. Overall, the branch performs most of its functions well. However, improvements are needed in inventory and budget management.

Inventory

Although inventory discrepancies have been within allowable limits, the processes for managing and tracking are poorly defined and documented. Many of SIO's shared services were transferred to the Bureau of Administration as part of the Center for Excellence effort. Inventory, however, has remained a SIO responsibility, requiring SIO to account for and manage its hardware and software inventory while coordinating with the Bureau of Administration as needed.

For the hardware inventory, each of the five SIO divisions has its own primary area custodial officer, with the ESOC division having several because of its multiple locations. Each area custodial officer performs a check of the hardware inventory each year and reports the information to branch staff members, who consolidate the inventory information and send it to the Bureau of Administration for uploading to the Integrated Logistics Management System. Branch staff began drafting property management standard operating procedures in August 2011. However, the document is still not final and does not provide a clear definition or explanation of what constitutes "hardware" to be included in SIO's inventory records. The OIG team also learned of discussions to separate the ESOC inventory from the rest of SIO for better accountability; however, the OIG team did not see corresponding decision documents or a note of such plans within SIO's standard operating procedures.

Recommendation 10: The Bureau of Information Resource Management should revise and finalize the property management standard operating procedures for the Systems and Integration Office to provide clear definitions for and identification of division and individual responsibilities. (Action: IRM)

Hardware inventory tracking also warrants attention. Currently, area custodial officers are conducting inventory reconciliation for their respective divisions and forwarding this information to assigned staff members. However, neither BEC nor the rest of SIO uses a centralized tool to track its inventory information internally. Instead, staff is using paper or an old version of a utility within IRM's Remedy IT Service Management suite to track inventory information. Because there is no consistent tracking mechanism, some of SIO's inventory items are missing. For example, during the course of the inspection, area custodial officers spent several weeks performing "floor sweeps" looking for missing items. At the end of the initial reconciliation period, SIO reported to the Bureau of Administration more than $275,000 in missing equipment. Although this amount is less than the 1 percent allowed by Bureau of Administration requirements, several of the items cost more than $5,000 each, requiring SIO to report the discrepancies to the Department's Property Survey Board for action. A more concerted effort of inventory oversight and accounting by SIO would help resolve this problem.

Recommendation 11: The Bureau of Information Resource Management should implement a tool for the Systems and Integration Office to track its inventory. (Action: IRM)

The software inventory process is a work in progress for SIO. Each SIO division used to handle its own software ordering, receiving, and licensing processes. SIO management decided to consolidate those activities under BEC and, in the process, identified a problem with expired software licenses. BEC management has been reviewing the issue in two phases. The first includes documenting the "as is" environment for software. The second entails documenting the "to be" environment, selecting a tool to track licenses, creating a workflow diagram, and revising the existing standard operating procedure. The OIG team obtained a copy of the developed workflow diagrams explaining the current "as is" process for ordering and receiving software and found it to be detailed and clear. SIO management is working toward a method for tracking software licenses, and the OIG team supports its efforts in this regard.

Budget

SIO is not using set criteria or guidelines for financial decisionmaking. The Planning, Acquisition, and Budget branch manages SIO budget activities. Currently, SIO is operating under a continuing resolution; however, it did submit a budget request for more than $82 million for FY 2013. BEC management attends weekly budget meetings with representatives from IRM. However, the OIG team attended several of these meetings and found the discussion to be unfocused and unclear. Lack of clarity from IRM has led to SIO's development of its own internal approval process to track funding requests—the financial CCB.

As part of this internal SIO process, employees submit funding requests for training and purchases to their respective branch and division chiefs for review and approval. Requests are entered into CEIS and then exported by the BEC division chief into a spreadsheet every week for the SIO senior staff meeting. The SIO director and division chiefs, which form the financial

CCB, review purchase and training requests and approve or reject them. Approved requests are placed onto a purchase fund request form and submitted to IRM senior management for final approval and action.

The internal financial CCB process is a useful management tool for setting priorities. However, no set criteria or guidelines are used by management for decisionmaking. As a result, there is no clear rationale for approving or rejecting requests. [redacted]

Recommendation 12: The Bureau of Information Resource Management should develop a set of criteria and guidelines for the Systems and Integration Office's financial change control board to use in its review of and decisions on purchase and training requests. (Action: IRM)

A contractor within the branch handles SIO's budgeting, which is typically an inherently governmental function. This individual is responsible for and privy to the full spectrum of information on budgeting, funding requests, and pending contracts for SIO activities. Although BEC management has commented that SIO management approval is needed before any budget action, the OIG team is concerned about potential conflicts of interest and lack of independence in budgeting activities. The contract company employing this individual accounts for a large portion of SIO contractor staff in operational fields. Granting this contractor access to all budget information could thus afford his company an unfair advantage on future opportunities. Further, the risk of losing institutional knowledge is possible with such heavy reliance on one contract employee to compile budget information and attend meetings on behalf of SIO.

Recommendation 13: The Bureau of Information Resource Management should reassign the responsibility for monitoring and tracking of and accounting for budget information in the Systems and Integration Office to a government full-time employee and make only limited budget information accessible to contractor staff. (Action: IRM)

Information Management Support Branch

The Information Management Support branch, a team of four individuals, handles the development and management of the Project Tracking System, as well as SharePoint waiver requests. The Project Tracking System uses Microsoft Project Server to fulfill two purposes—tracking the time and attendance for contract staff and assisting with project management for SIO projects. Use of the system for project management is not mandatory, but the SIO director has advised employees to use it for their respective projects. More discussion on the Project Tracking System and its linkages to the SDLC process is provided in the Executive Direction section of this report. The responsibility for SharePoint waiver requests, however, could be better aligned within another SIO division.

SharePoint Waiver Requests

The CCS division used to handle SharePoint waiver requests; however, two employees in the BEC division are now responsible for this function. Posts or bureaus submit waiver requests

to establish a local SharePoint environment primarily because the centralized SharePoint platform does not perform well at posts that have low bandwidth or high network latency. The requesting post or bureau completes a waiver form and submits it to SIO, which then passes the form to IRM's Enterprise Network Management office for latency analysis. The regional bureau's executive director approves the cost and personnel resource allocation to support the waiver and then forwards the form to SIO for final recommendation and action. According to staff members, the latency analysis performed by IRM's Enterprise Network Management office drives the decision on SharePoint waivers. Since 2009, SIO has received a total of 54 requests, with 40 receiving approval. The number of waiver requests processed is minimal and could easily be reassumed by the CCS SharePoint team without burdening staff. Centralizing all SharePoint functions within CCS would provide decisionmakers with the most current information on upgrades and schedules.

Recommendation 14: The Bureau of Information Resource Management should reassign the responsibility for the management and analysis of SharePoint waiver requests to the Collaboration and Compensation Services division within the Systems and Integration Office. (Action: IRM)

Enterprise Server Operations Center Customer Management Branch

The ESOC Customer Management branch, a team of three individuals, works under the coordination of BEC staff on the development and updating of ESOC SLAs and recently assumed responsibility for participating on the Department's IT Change Control Board and performing an analysis of Remedy tickets on behalf of SIO. Because ESOC is better positioned to handle its own SLAs, it makes sense to transfer overall responsibility for this function from BEC to ESOC personnel.

Service Level Agreements

BEC staff members coordinate the development and updating of SLAs, which includes 129 active agreements and 67 up for renewal. ESOC SLAs are provided to Department bureaus or offices as part of the data center consolidation of their servers and networks. Generic SLAs are provided to each customer, with attachments detailing specific information pertaining to the operational support and setup for that particular bureau or office.

BEC staff commented that the ESOC SLA process needs improvement and has been working with ESOC personnel on developing a workflow document. Specifically, BEC staff noted lack of clarity on the divisions' respective roles and responsibilities and on the point at which BEC and ESOC staff become involved in the SLA process. This became an issue when new Department customers started contacting ESOC personnel for consultation, and ESOC informed BEC staff as an afterthought. ESOC personnel are now regularly informing BEC of their discussions with new customers so that the latter can prepare any necessary documents. It is understandable why customers would seek information from ESOC personnel, as they handle the operational support for the bureau as part of the data center consolidation. Because ESOC personnel have daily involvement with data center consolidation activities, they are also better equipped to answer any questions or inquiries from existing or new customers. Further, ESOC

staff can provide customers with information on storage capacity, operational support levels, and timelines. For these reasons, it makes sense for ESOC to take responsibility for its SLAs.

Recommendation 15: The Bureau of Information Resource Management should reassign the responsibility for Enterprise Service Operations Center service level agreements to the Enterprise Service Operations Center division within the Systems and Integration Office. (Action: IRM)

Enterprise Server Operations Center Divisions

ESOC consists of two divisions—O&M and D&B. The O&M division provides around-the-clock operational and maintenance support for the Department's domestic data centers, and the D&B division assists with the architecture, modernization, and expansion of Department IT facilities by standardizing IT processing resources such as servers, databases, and applications.

The ESOC divisions are well managed by their division chiefs and staff. Processes are in place to handle everyday tasks, contingencies, and any crisis that might arise. ESOC is performing data center consolidation in accordance with the Federal Data Center Consolidation Initiative. ESOC is also moving the Department toward greater virtualization, both domestically and internationally, in conjunction with the IRM Global Information Technology Modernization program. Further, ESOC is leveraging those virtualization and data center consolidation efforts to move the Department toward cloud computing, which is defined and discussed in detail in the Cloud Computing section of this report.

Operations and Maintenance Division

The O&M division manages the operational domestic data centers. ESOC East is primarily a contractor-owned and -run facility that requires Department oversight of the building; heating, ventilation, air conditioning, and electrical services; and management of the servers and rack space. ESOC West, meanwhile, is nearing completion on the western power grid. It is owned and operated by the Department, including facilities management; heating, ventilation, air conditioning, and electrical services; and all servers located in the data center.

ESOC currently provides operational support to 28 bureaus and offices and manages approximately 5,043 servers. Customers include large stakeholders such as the Bureau of Consular Affairs and smaller customers with only one or two servers. The type of support provided by ESOC could be one of five options ranging from "colocated," which includes minimal oversight, to "managed," which requires ESOC to manage all hardware and operating system maintenance. At overseas posts, and in conjunction with IRM's Global Information Technology Modernization program, ESOC is working on combining multiple infrastructure servers into a local virtual infrastructure. Virtualization allows multiple servers to be hosted on one piece of hardware—thus saving energy, space, and cooling. This project is on schedule for completion in FY 2015.

SIO has implemented a process of SLAs to ensure quality customer service. As stated earlier in the report, a generic SLA is customized with amendments for each customer to describe the respective bureaus' or offices' setup and level of support to be provided. The SLAs require the O&M support desk to respond to an ASG-Sentry alert (a server monitoring service) within 10 minutes. The ESOC local area network administrator remotely checks the server, notifies the customer by email within 15 minutes or by phone within 30 minutes, and begins troubleshooting the outage. The ESOC local area network administrator is required to be on site within 90 minutes from the initial notification. The typical stakeholder's SLA requires O&M to meet these markers 90 percent of the time. The CEIS trouble ticket monitoring system demonstrated that O&M has been meeting its SLA requirements 97 percent of the time during

the past year. However, CEIS also shows 28 percent of servers as "unknown" in status, indicating there are no SLAs in place governing the management of those servers.

The Department began a data center consolidation program in 2002 to support the Department's global IT infrastructure. The Department was well along on this effort by the time the Federal Chief Information Officer kicked off the Federal Data Center Consolidation Initiative in February 2010, which requires agencies to perform asset inventories and create a data center consolidation plan. The Department had initially conducted an asset inventory in 2007, prior to the Federal Data Center Consolidation Initiative mandate. The latest update shows that enterprise applications and network services for supporting worldwide Department objectives are enabled by more than 5,000 servers located in 12 data centers in the United States. Currently 42 percent of all domestic servers have been virtualized. The Data Center Consolidation goals include consolidating, optimizing, and decommissioning more than 70 percent of the data centers by FY 2015. ESOC is on track to achieve those goals.

During the inspection, the OIG team observed that not all servers and network devices in the data centers have complete labels. The servers managed by O&M are labeled properly, whereas servers colocated with, [redacted]

Informal Recommendation 2: (b) (5) [redacted]

The data centers designed and managed by ESOC meet all physical and security requirements (b) (5) [redacted]

Informal Recommendation 3: (b) (5) [redacted]

Legacy Support Branch

The Department has been migrating away from the legacy mainframes to open systems computing[1] for the past decade, and consequently the need for legacy mainframe computers and staff is fast disappearing. The move by private industry and the Department away from mainframe computing to open systems has been customer driven. Some of the prominent Department mainframe applications supporting financial, retirement, and consular operations have already migrated during the past 5 years. The two remaining major mainframe applications are the Bureau of Resource Management's Consolidated American Payroll Processing System (CAPPS) application and the retirement records system, which are expected to be migrated by the end of 2013 or beginning of 2014. As mentioned earlier in the Collaboration and Compensation Services Division section of this report, this migration will eliminate the need for the payroll support function.

The significant decrease in the Department's overall number of mainframe applications has resulted in ESOC's having a larger capacity mainframe computer and more employees than it needs to support operations. In an effort to save money and better align the scope of operations with the Department's needs, SIO management acquired a smaller mainframe computer and reassigned or eliminated its contract employees.

Developing a workable solution for ESOC's 13 full-time employees in the Legacy Support branch has been difficult; however, ESOC management has tried to upgrade the technical skills of operations staff members so that they can transition to positions requiring knowledge of newer technology. Toward this end, ESOC management developed a training plan to provide the Legacy Support branch staff with details on the technical skills necessary to be effective with the newer open systems. The ESOC open systems training plan was patterned after the Foreign Service Institute's IT training program, which requires students to meet certain course prerequisites before being eligible for the next, progressively more difficult course. At the end of the training period, individuals would, in theory, have the necessary understanding and skills to be competent and ready to work with open systems.

Since implementing the training plan, SIO has experienced budget cuts resulting in limited availability for staff to attend classroom courses. However, ESOC management continues to encourage Legacy Support branch staff to attend courses and makes their doing so a priority. ESOC management has also instituted a small pilot program to give a few ESOC Legacy Support branch staff members an opportunity to work with open systems as a first-level help desk staff member. The OIG team encourages ESOC management to continue to provide such opportunities to the Legacy Support branch.

Design and Build Division

The D&B division is led by an effective division chief with a strong technical background. The division chief's focus during the inspection was the standup of a new enterprise

[1] Open systems are defined as a class of computers and associated software that provides some combination of interoperability, portability, and open software standards. The open system standard used by the Department is based on the Microsoft Windows operating system.

data center—ESOC West. In his absence, most day-to-day management responsibilities for the ESOC D&B division were handled by the other ESOC division chief.

The D&B division manages the design and building of the ESOC data centers, oversees implementation of the Federal Data Center Consolidation Initiative, and provides enterprise-level Tier III technical support. The D&B division has four areas of responsibility, each one managed by a technical team lead. These four areas include virtual infrastructure, network, backup and recovery, and monitoring and access. Each technical team lead manages and provides technical oversight for his or her assigned contract staff. The four technical teams work in a collaborative manner with ESOC customers to ensure that systems being migrated by or operating in ESOC have adequate processing capability and sufficient disk storage and are backed up and monitored appropriately. In addition to the four teams, the division has a Project Management branch and a Cloud Services branch. The Project Management branch coordinates communication between the four technical teams (lanes), and the Cloud Services branch focuses on the development of cloud services internal to SIO.

Customer and Executive Information System

CEIS has become an integral part of ESOC operations and has assisted the division in serving its customers. The CEIS application is a custom-built, integrated system that is a central collection point for all ESOC activities, including asset and configuration management, project tracking, and management reporting. CEIS also continues to play a critical role in helping SIO provide status updates regarding its compliance with the Department's Federal Data Center Consolidation Initiative.

The CEIS application contains system owner information and technical details on the thousands of applications and systems that run in ESOC. The database also stores monitoring information from the various customer applications and uses this information to automatically identify problems as they occur as well as potential problems that might occur.

Unlike the Department's Remedy help desk application, CEIS is proactive in that it uses the monitoring information as a trigger to generate an automatic escalation process to alert ESOC staff or the customer of a reportable condition, which is often tied to the customer's SLA and to ESOC's escalation procedures. Typically, ESOC staff can alert a customer in less than 10 minutes after an incident occurs. The CEIS workflow escalation process includes information to guide the ESOC technician through the steps to troubleshoot and resolve a problem.

Cloud Computing

The notion of cloud computing has been a topic of conversation in the IT field for several years now, and though many might have difficulty defining it clearly, that uncertainty has not stopped budgets from bending to accommodate the technology's early adopters. The Department shares that uncertainty over what type of cloud environment to pursue, how much to invest, who is responsible, and which rules to follow. Although SIO has done much innovative work in the spirit of cloud computing, its implementation of cloud computing at this point does not meet the requirements outlined in Federal guidance.

Cloud computing is generally regarded as the delivery of computing capability as a service rather than a product, much like the difference between purchasing power from a utility company over the power grid and buying a generator. Cloud computing is often distinguished further from the utility analogy by describing the software as a service model, wherein the customer has no knowledge of or control over the underlying technology infrastructure supporting the service. NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing has been a focal point in the Federal government for several years because of its vast potential for creating economies of scale across Federal agencies and for realizing cost savings. It has been advanced by efforts such as the Cloud First Policy and, more recently, by the Federal Chief Information Officer in a memorandum to agency chief information officers in December 2011, directing them to use the Federal Risk and Authorization Management Program to identify and select vetted cloud service providers. NIST has also provided guidance on implementing Federal cloud computing requirements within NIST SP 800-45.

In the Department, cloud computing has featured prominently as a goal in the IT Strategic Plan and in the previous IRM Bureau Strategic and Resource Plan. IRM's Strategic Planning Office is leading Department efforts to plan a cloud computing strategy. The main flash point in that discussion revolves around the extent to which the Department commits to cloud computing—whether it will consist of an internally built and maintained "private cloud," or whether the Department purchases computing services from an external provider in the "public cloud," or some combination thereof. SIO would be responsible for implementing the Department-wide private cloud environment.

Systems and Integration Office Implementation of Cloud Computing

In an effort to realize the benefits of cloud computing, SIO has pursued a private cloud environment for its customers, which is similar to many other Federal agencies and corporations. The consolidation of the Department's individual data centers into enterprise-level data centers as part of the Federal Data Center Consolidation Initiative fulfills many of the overarching cloud computing goals laid out in the Cloud First Policy and the previous IRM Bureau Strategic and Resource Plan. These goals include improved asset utilization, aggregated demand, and improved network and application. However, as it stands today, SIO's implementation does not fulfill the characteristics of a cloud computing environment as defined by NIST, which has developed a model that includes five essential characteristics of a cloud environment, four alternative deployment models, and three alternative service models.

The five essential characteristics that define a cloud environment are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. ESOC does not fully satisfy any of these characteristics. Although ESOC customers can make limited changes to their application and configuration, they cannot make changes automatically to their server or network storage without ESOC assistance (on-demand self-service). The customer does not yet have the capability of accessing ESOC systems from a variety of computing platforms,

such as thin clients, tablets, or mobile phones (broad network access). The ability to pool resources and automatically reassign computing resources according to consumer demand does not exist within ESOC (resource pooling). The capability of adding and releasing computing resources commensurate with demand without ESOC intervention does exist to some extent (rapid elasticity). Although ESOC has some capability to monitor and use a monitored value to alert a customer of a problem, the value cannot be used automatically to control and optimize resources (measured services).

The deployment model attribute refers to the cloud customer base. Because the ESOC infrastructure is exclusively for the Department's domestic customers, the implementation of an ESOC cloud would thus be considered private. The other attribute used in the NIST cloud definition is the service model. Because ESOC customers have some capability to modify their computing resources within the Department's security guidelines and ESOC's processes, the type of service model used by ESOC is called "infrastructure as a service."

Even in the case of a private cloud, NIST's essential characteristics are still applicable and serve to define those traits that make pursuing a cloud environment worthwhile, even if only to a degree. The appropriate measure of applicability is discovered through strategic planning. Within SIO, if the focus is to remain on the private cloud, this should be made clear in its mission statements and elaborated on more in the next Department IT Strategic Plan and the next bureau strategic planning request. Ultimately, the development and implementation of a Department-wide cloud architecture will require close coordination among IRM and other Department offices to ensure a vision that is consistent with Department-level strategic plans. Be the cloud public or private, it would be advisable for senior IRM management to review the NIST model as given in NIST Special Publication 800-145 to ensure that the Department's cloud computing goals are consistent while ensuring appropriate security controls and compliance with Federal requirements.

Recommendation 16: The Bureau of Information Resource Management should incorporate the essential characteristics of cloud computing as specified by the National Institute of Standards and Technology model into its cloud computing efforts to facilitate consistency among mission statements and goals. (Action: IRM)

Collaboration and Compensation Services Division

The CCS division successfully maintains systems that perform some of the more vital services in the Department, despite the juxtaposition in one division of state-of-the-art collaboration tools with some of the more outdated legacy technology still in use. CCS is responsible for two enterprise-level programs—SharePoint and CAPPS. The division's efforts with SharePoint have brought new methods of information sharing to the Department and in some cases revolutionized office workflow processes. This achievement has had some unintended consequences as offices have relied on SharePoint to an unexpected degree. Meanwhile, the payroll function has been reliably and consistently dispatched but faces an uncertain future in CCS as transition plans loom. Overall leadership at the division and branch levels is strong, and staff members share a sense of camaraderie and enthusiasm for their work.

Division staff includes 71 individuals: 10 Civil Service employees, 2 Foreign Service employees, and 59 contractors within two branches—Enterprise Collaboration Services and Compensation Applications. The Enterprise Collaboration Services branch has a staff of 50 and is responsible for supporting SharePoint operations, whereas the Compensation Application branch has a staff of 18 and supports CAPPS. CCS has had long-term difficulties in staffing the Enterprise Collaboration Services branch chief position. Although the position was filled in August 2011 after a lengthy vacancy, the incumbent has since been promoted within the SIO organization and the position is once again vacant. The CCS division chief has raised with SIO management the importance of and need for filling the branch chief position.

Enterprise Collaboration Services Branch

The Enterprise Collaboration Services branch provides custom development and technical support for SharePoint, as well as customer support at the Tier II and Tier III levels. SharePoint is a multipurpose Web application used for online collaboration, content management, and workflow processing. The branch's main focus is managing and supporting SharePoint services. The division chief is well regarded among staff members for her leadership, focus, and approachability. The equally engaged branch chief has set high standards of performance in a professional manner to complete tasks and goals. Individual and group meetings help to keep everyone informed and allow staff to express ideas. Staff members have a sense of camaraderie, and morale is good in spite of uncertainty about the potential effect of the Vanguard contract.

SharePoint Program

SharePoint began as a State Messaging and Archive Retrieval Toolset pilot initiative and transitioned to SIO in 2008. SharePoint was designed as a knowledge management platform to facilitate information sharing and collaboration among bureaus and offices. However, the use of SharePoint has grown significantly beyond its intended scope, as demonstrated by the increase in the number of SharePoint sites from 208 in 2008 to more than 25,000 in 2012. To date, the Department has spent more than $15.6 million on SharePoint development and implementation. According to SIO management, the application has become a mission-critical tool, with many

Department officials using SharePoint to conduct daily business as well as support key political and military events.

The SharePoint program is deployed on OpenNet, ClassNet, and SIPRNet, as well as on the Internet to create public-facing Web sites. The consensus is that SharePoint was never intended to be a mission-critical application. The planned and implemented deployment of SharePoint has been based on its use as a collaboration tool. However, over time, bureaus have become increasingly more dependent on the application, to the point where many now automate workflow processes—their day-to-day tasks—through SharePoint. Such extensive usage, where any downtime can affect a bureau's ability to fulfill its mission, means that SharePoint has essentially become mission critical to these entities. It is thus time to reevaluate risk assessments and other terms and conditions that were party to any SLAs entered into by SIO and its customers. Actions to remedy any shortcomings identified would follow, such as increased security controls or resources, as well as a new understanding on the part of customers as to what level of availability and customer service they really need and what level of customer service support CCS can actually provide. Such a discussion might also inform any future plans for a cost model.

From an information security standpoint, a reevaluation would involve revisiting the Federal Information Processing Standard's 199 categorizations assigned to SharePoint. For Federal Information Security Management Act purposes, SharePoint is treated as a series of Web sites and therefore as a part of each general support system. In the case of OpenNet, SharePoint inherited the same moderate security categorization that was assigned to OpenNet—resulting in enterprise SharePoint administrators and site collection managers being required only to implement security controls for the application that are consistent with a moderate categorization, despite the high reliance certain entities within the Department have on the application to conduct their daily business. Further, the documentation submitted to the IT asset baseline, the application that maintains the official Department inventory of systems for reporting to the Office of Management and Budget, is rather sparse. There is no mention of a parent-child reporting relationship between OpenNet as a general support system and SharePoint as merely Web sites hosted on that system.

Recommendation 17: The Bureau of Information Resource Management should perform a risk management assessment of SharePoint and determine the appropriate security categorization based on its current scope and use. (Action: IRM)

Another important consideration is that the use of SharePoint is dynamic and that risk management assessments can be valid only for a specific point in time. Customer behavior and usage of SharePoint will continue to evolve beyond the stage at which the risk assessment is performed, as evidenced by the wide proliferation of site collections. To handle that growth and provide better service according to multiple levels of mission criticality, SIO is already planning to create multiple server farms capable of meeting the different requirements as part of their SharePoint 2010 migration. However, customers could potentially still create sites and store content on those sites that is above the security categorization level at which the farm is accredited. Therefore, it will be important to ensure that site collection administrators and business owners certify their understanding of the categorization level of each SharePoint farm and the specific limitations on content within the SharePoint environment.

Recommendation 18: The Bureau of Information Resource Management should revise the service level agreement process for SharePoint services to include a signed certification of understanding from both parties regarding the current security categorization of SharePoint and the specific limitations on content within the SharePoint environment and implement a process for periodic review of the agreement. (Action: IRM)

Customer Support

Customer support for SharePoint gets mixed reviews from customers, largely because this function is shared between the Enterprise Collaboration Services branch and the IT Service Center (ITSC)—the single point of contact for all Department-wide IT support for consolidated bureaus. ITSC is responsible for issuing, logging, and tracking a ticket for each incident, as well as for posting notices about SharePoint outages. ITSC attempts to resolve the problem at the Tier I support level. If unsuccessful, ITSC transfers the issue to CCS, which handles Tiers II and III customer support levels. ITSC notifies customers of scheduled and unscheduled outages upon receipt of a CCS-generated email with the outage notification information. CCS also follows up with a phone call to ITSC about the email. ITSC allows a 90-minute window for sending emails with notification alerts, which has lead to customer complaints about system outages due to the lack of a timely notification. The process is cumbersome and inefficient. Any delay in communicating an outage, especially an unscheduled one, affects customer operations and reflects poorly on IRM customer service.

Recommendation 19: The Bureau of Information Resource Management should transfer the primary responsibility for notifying customers on SharePoint outages from the Information Technology Service Center to the Systems and Integration Office and revise the operational level agreement accordingly. (Action: IRM)

CCS has updated its internal standard operating procedures for ticket processing, system outages, and communication with ITSC. CCS has begun revising the 2009 operational level agreement between ITSC and CCS. The agreement describes the roles and responsibilities of all relevant parties and explains the procedures for providing technical assistance on SharePoint-related issues. The proposed changes will define the scope of CCS services to help reduce the number of misrouted tickets and includes reference links to a customer support site to help ITSC respond to common requests/incidents. CCS has not yet discussed the proposed changes and updates to the operational level agreement with ITSC; as a result, both parties are working from different procedures and processes.

Recommendation 20: The Bureau of Information Resource Management should revise the operational level agreement for SharePoint to delineate the roles and responsibilities of and procedures to be followed by the Systems and Integration Office and the Information Technology Service Center. (Action: IRM)

SharePoint customers are frustrated by the team's inability to correct problems in a timely manner. The OIG team was unable to determine the root cause of this issue because of the numerous components and parties involved in the operational aspects of the SharePoint environment (e.g., ITSC, CCS, and connectivity and latency factors). However, the inspectors advised CCS management to continue to perform customer outreach and make customer service

its top priority. In March–April 2011, the SharePoint team conducted a customer survey tailored to identify customer requirements for needed enhancements in SharePoint. However, the survey did not contain any general customer service questions except for one on the SharePoint customer support site where CCS advertises its brown bag sessions and workshops. Lack of adequate customer feedback hampers SIO's ability to address issues of primary concern to end users.

Recommendation 21: The Bureau of Information Resource Management should conduct regular SharePoint customer service surveys to seek feedback on the timeliness of responses, routing of tickets, resolution of issues, and functionality of the application. (Action: IRM)

Once ITSC closes a ticket, it issues surveys to its customers to request feedback. In the past, ITSC provided this information to bureaus and offices. The Enterprise Collaboration Services branch only recently began asking for this information because of the OIG inspection. The branch received 109 responses on SharePoint usage from January 2011 to March 2012, during which time the branch processed 2,982 tickets. CCS realizes the benefit of receiving this information and has begun analyzing and measuring it against SLAs. For example, the group is reviewing how long it takes for tickets to be transferred from ITSC's Tier I support level to CCS. The OIG team encourages CCS's continued efforts to analyze performance and problem areas.

CCS has hosted more than 50 Enterprise SharePoint Configuration Control Board meetings since August 2008. Five of those meetings were recently conducted virtually. During the meetings CCS shares the status and impact of proposed configuration changes, reports on the status of past or future maintenance activities, and provides an opportunity for SharePoint users to raise issues and ask questions. As of January 2012, CCS had decided to hold virtual and in-person meetings. The virtual meetings were intended to provide convenience to those overseas customers in different time zones but instead have proved to be a disadvantage, as they hinder back-and-forth communication with the SharePoint team. The SharePoint community is now engaged in discussions about whether to continue virtual meetings.

SharePoint 2010 Migration

The Enterprise Collaboration Services branch has been working extensively on the migration to SharePoint 2010. According to SIO management, SharePoint 2010 will provide users with enhanced functionality, improved search capability and performance, and increased storage capacity. The migration to SharePoint 2010 requires extensive planning and coordination among parties, as it involves moving all site collections from the SharePoint 2007 platform. The branch originally planned to deploy the pilot in October 2011 but admits that this deadline was too optimistic. According to management, several factors have contributed to the missed milestone for the pilot, including performance problems with SharePoint in fall 2011, the vacant branch chief position, staff turnover in the lead contract project manager position, and increased workload among engineering staff members in resolving Tier III support issues. The branch has now reset the pilot deployment date to May 2012, with an estimated year to migrate all customer data. To assist, staff is employing a Scrum team software development methodology to expedite the prototyping of a pilot architecture. Further, when SIO filled the branch chief position, albeit briefly, in August 2011, CCS was able to prioritize projects and refine processes.

SIO management is in the early stages of determining whether and how to charge customers for SharePoint services. CCS is responsible for designing a cost model and completing a formal analysis so that it can present an informed recommendation to senior management on the various fee-for-service options. Currently, CCS charges a fee of $135 per hour for any site design work it conducts beyond the 8 hours of support it provides to customers. The proposal to begin charging for additional SharePoint services and usage is a recent one, and senior IRM management requested that CCS management determine a charge-back cost model for SharePoint support services.

Recommendation 22: The Bureau of Information Resource Management, in coordination with the Bureau of Resource Management and the Bureau of Administration, should identify the appropriate funding mechanisms and payment structures, if any, for SharePoint usage and share this information with SharePoint customers. (Action: IRM, in coordination with RM and A)

Compensation Applications Branch

The Compensation Applications branch maintains the 30-year-old CAPPS mainframe, which generates payroll for all U.S. citizen Department employees. The branch has performed this mission-critical function well but is in transition as the Department plans to sunset the current CAPPS application and move the payroll function to the Bureau of Resource Management. This change has widespread ramifications for SIO, which still has much to do to prepare for the transition.

The CAPPS system makes payments to approximately 29,500 Foreign Service and Civil Service employees, family members, and personal services contractors. CAPPS excludes Foreign Service national employees, who are paid by Foreign Service National Payroll Operations at Global Financial Services Charleston, which is responsible for managing and overseeing the Department's payroll operation and for directing the Compensation Applications branch by establishing priorities and providing guidance on mandated projects, such as the Roth Thrift Savings Plan program, that the branch must implement. Global Financial Services Charleston also certifies the accuracy of payroll, funds CCS operations, and reviews the American personnel and payroll history contained in the CAPPS Retirement Record System—the repository of current and historical master files used to calculate the basic retirement benefits payable to separated employees.

Discussions about modernizing the payroll system have been ongoing since 2004 but gained added momentum when the Department decided not to join one of the Office of Management and Budget's designated e-Payroll service providers. Instead, the Department is planning to develop a replacement payroll system that the Bureau of Resource Management will deploy by the end of 2013. The sunset of the CAPPS system will mean the abolishment of Compensation Application branch operations and uncertainty for its staff. The division chief has known about these plans since November 2009 but has yet to develop a transition plan for branch staff. A February 2012 visit by the Global Compensation Operations manager confirmed that the transition to the new payroll system is on schedule for a December 2013 deployment. After the transition, the Compensation Application branch staff will be responsible only for maintaining the Department's domestic time and attendance system, WebTatel, until Global Financial

Services Charleston deploys a new system for domestic payroll processing, tentatively planned for 2014.

The CCS division chief has encouraged its seven team members to prepare themselves for the transition by offering training and asking staff to consider other possible career directions. Some of these individuals have done little to prepare, and those with outdated technological skills may be challenged in today's sophisticated IT world. Individual development plans for the Compensation Applications branch staff are being updated. CCS division management has delayed development of a transition plan because of uncertainty regarding how the Vanguard contract will affect the payroll function. However, during the OIG inspection, management decided that the payroll function will not be part of the Vanguard 2.3.x series and that the contract will continue through its final option year. A transition plan will assist management and staff to adjust to the change in responsibilities and the role of the branch as a whole. The Department's procurement experts can help SIO define the best course of action to continue providing contractual support when the current contract expires in September 2012 and until the Bureau of Resource Management takes control of the payroll function.

Recommendation 23: The Bureau of Information Resource Management, in coordination with the Bureaus of Resource Management, Administration, and Human Resources, should develop a transition plan for the Compensation Applications branch that includes, at a minimum, an assessment of skills and training needs for individuals and a determination of the post-transition role of the branch. (Action: IRM, in coordination with RM, A, and DGHR)

Recommendation 24: The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should determine what contractual arrangements are necessary to administer the payroll function pending its transition to the Bureau of Resource Management's portfolio and implement them accordingly. (Action: IRM, in coordination with A)

Enterprise Programming and Integration Division

The EPI division is focused on facilitating Department-wide accessibility to software solutions by employing application integration and data management technology solutions and services. EPI is the focal point for some of the Department's enterprise applications such as eCountry Clearance, WebPass, and Concierge. The division chief received favorable marks from staff, with many acknowledging the welcome structure and accountability she has brought to the division. Most of the EPI branch chiefs and project managers are new to the Department, so a transition is still under way regarding the SDLC process. Management oversight of contract employees and their work is an area of concern.

A total staff of 17 full-time employees and 74 contractors support EPI's four branches: Data Management, Integrated Projects, Application Development, and the Program Management office. The division chief and branch chiefs meet regularly to discuss project status and provide suggestions to one another on internal processes.

Data Management Branch

The Data Management branch is working effectively as a team, receiving strong leadership from its branch chief. The team consists of 3 full-time employees and 17 contractors who are responsible for treating data that are shared across bureaus within the Department as a global asset and for handling data governance matters. Two sections make up this branch—Enterprise Data Warehouse and Data Management and Governance. Each section engages with its customers to define business and data standards.

The branch chief meets with staff on a regular basis and is considered to be approachable, which has helped the branch address difficult issues. For example, the branch was involved in discussions with one of its primary customers regarding the implementation of WebPass and Concierge. Lack of participation from senior IRM officials caused problems initially, which the branch has since overcome with frequent communication between the branch chief and the customer.

Integrated Projects Branch

With a team of 3 full-time employees and 17 contractors, the Integrated Projects branch provides support services for CEIS and handles all of the Tier II and Tier III customer support levels for the Enterprise Service Bus, IT Asset Baseline, and Tips of the Day. The branch chief joined SIO 5 months ago and has been working on developing reporting and operational processes. The branch is utilizing the Project Tracking System and internal spreadsheets to document its work.

The branch chief is an advocate for adhering to the established chain of command within management. As a result, all information is filtered through proper management channels from contractors to government project managers to the final report to the branch chief. This process helps keep government project managers informed of the work their respective teams are

performing. The branch chief also takes a proactive approach, as evidence by his enrollment of himself and other full-time personnel in COR training to improve monitoring of contractor work.

The OIG team found that information was missing from records for those applications and systems under EPI's purview as an application owner, including in required fields such as the profile, distribution, parent-child relationship, and Federal enterprise architecture mapping. There were also apparent differences in how much information was reported for new applications and systems versus legacy assets. According to EPI management, stand-alone applications and systems that will reduce or eliminate the dependencies of other systems and subsystems with parent-child relationships are under development. However, there was no description of what information to include for each application and system, nor an indication of whether management had approved these decisions. During this inspection, EPI management provided the missing information for its applications within the IT Asset Baseline.

Application Development Branch

The Application Development branch has 6 full-time employees and 26 contractors who are responsible for developing and supporting enterprise applications such as eCountry Clearance, WebPass, and Concierge. The OIG team found the branch chief less than fully engaged in the work or personnel matters of the branch. Although the chief meets with staff weekly, the level of engaged conversation is limited. When the OIG team brought these matters to the branch chief's attention, his response was not supportive of needed change.

In addition, the branch chief has given more authority to contractors than to government full-time employees. For example, contractors are engaging as points of contact for and holding meetings with customers in lieu of government project managers. The OIG team was told repeatedly of instances in which contractors were not sharing information appropriately with government project managers and were assigning tasks to full-time employees only with the branch chief's permission. Contractor management is discussed further in the Executive Direction section of this report.

The EPI division chief became unaware of these problems only during the OIG inspection. Once informed, the division chief began to make organizational changes to ensure proper oversight of contractor and supervisory authority, including designating one full-time employee as the government lead for the application support help desk. The contractor lead will remain responsible for managing the contract staff with regard to applications support. The branch chief is also establishing recurring status meetings with all government leads to monitor the activity and productivity of full-time employee government staff on the application support desk.

Program Management Office

The Program Management office has a team of 3 full-time employees and 14 contractors and is responsible for the oversight and development of the project management process flows and IT security and compliance within EPI. One of the team's primary areas of focus is the integration of best practices and efficiencies within programs such as WebPass and Concierge. Among the office's accomplishments is the establishment of EPI's well-documented SDLC,

which outlines and describes approaches to a variety of tasks or activities that take place during the software development process, from initiation to deployment. The responsibilities and role of EPI's Program Management office is similar to other program management and process improvement positions within SIO. See the Executive Direction section of this report for more details on this matter.

The Program Management office comprises four teams. The Program Management team meets with customers during the initiation phase of a project to gather requirements. The IT Security and Compliance team handles the information systems security officer and compliance functions, including certification and accreditation activities. The Release and Configuration Management team validates change control and deployment readiness documentation. Finally, the Architecture/System Administration team is responsible for developing the best solution to meet customer needs and requirements. See the Program Management Functions section of this report for further discussion of the Program Management office and a related recommendation.

List of Recommendations

Recommendation 1: The Bureau of Information Resource Management should establish a central repository for the management of Systems and Integration Office contracts so that all relevant documentation for each contract, such as statements of work, amendments, and invoices, are in one central location. (Action: IRM)

Recommendation 2: The Bureau of Information Resource Management should prepare a funding document that details the authorized, spent, and remaining funds for each Systems and Integration Office contract and implement procedures to verify and update this information regularly. (Action: IRM)

Recommendation 3: The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should assign the responsibilities of contracting officer's representatives and government technical monitors for Systems and Integration Office contracts to individuals who have the technical expertise to evaluate the scope of work performed by the contractors. (Action: IRM, in coordination with A)

Recommendation 4: The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should implement a policy requiring all assigned contracting officer's representatives and government technical monitors for Systems and Integration Office contracts to apply for Federal Acquisition Certification by completing the required training and submitting corresponding documentation to the Office of the Procurement Executive in accordance with Department of State guidelines. (Action: IRM, in coordination with A)

Recommendation 5: The Bureau of Information Resource Management should clearly document the alternative systems development methodologies and criteria for use of each methodology in Systems and Integration Office development activities. (Action: IRM)

Recommendation 6: The Bureau of Information Resource Management should document which tool to use for centralized project tracking for Systems and Integration Office projects and enforce compliance among personnel. (Action: IRM)

Recommendation 7: The Bureau of Information Resource Management should determine the role and organizational placement of the Program Management office and function within the Systems and Integration Office and define terminology pertaining to program management activities. (Action: IRM)

Recommendation 8: [redacted]

Recommendation 9: [redacted]

Recommendation 10: The Bureau of Information Resource Management should revise and finalize the property management standard operating procedures for the Systems and Integration

Office to provide clear definitions for and identification of division and individual responsibilities. (Action: IRM)

Recommendation 11: The Bureau of Information Resource Management should implement a tool for the Systems and Integration Office to track its inventory. (Action: IRM)

Recommendation 12: The Bureau of Information Resource Management should develop a set of criteria and guidelines for the Systems and Integration Office's financial change control board to use in its review of and decisions on purchase and training requests. (Action: IRM)

Recommendation 13: The Bureau of Information Resource Management should reassign the responsibility for monitoring and tracking of and accounting for budget information in the Systems and Integration Office to a government full-time employee and make only limited budget information accessible to contractor staff. (Action: IRM)

Recommendation 14: The Bureau of Information Resource Management should reassign the responsibility for the management and analysis of SharePoint waiver requests to the Collaboration and Compensation Services division within the Systems and Integration Office. (Action: IRM)

Recommendation 15: The Bureau of Information Resource Management should reassign the responsibility for Enterprise Service Operations Center service level agreements to the Enterprise Service Operations Center division within the Systems and Integration Office. (Action: IRM)

Recommendation 16: The Bureau of Information Resource Management should incorporate the essential characteristics of cloud computing as specified by the National Institute of Standards and Technology model into its cloud computing efforts to facilitate consistency among mission statements and goals. (Action: IRM)

Recommendation 17: The Bureau of Information Resource Management should perform a risk management assessment of SharePoint and determine the appropriate security categorization based on its current scope and use. (Action: IRM)

Recommendation 18: The Bureau of Information Resource Management should revise the service level agreement process for SharePoint services to include a signed certification of understanding from both parties regarding the current security categorization of SharePoint and the specific limitations on content within the SharePoint environment and implement a process for periodic review of the agreement. (Action: IRM)

Recommendation 19: The Bureau of Information Resource Management should transfer the primary responsibility for notifying customers on SharePoint outages from the Information Technology Service Center to the Systems and Integration Office and revise the operational level agreement accordingly. (Action: IRM)

Recommendation 20: The Bureau of Information Resource Management should revise the operational level agreement for SharePoint to delineate the roles and responsibilities of and procedures to be followed by the Systems and Integration Office and the Information Technology Service Center. (Action: IRM)

Recommendation 21: The Bureau of Information Resource Management should conduct regular SharePoint customer service surveys to seek feedback on the timeliness of responses, routing of tickets, resolution of issues, and functionality of the application. (Action: IRM)

Recommendation 22: The Bureau of Information Resource Management, in coordination with the Bureau of Resource Management and the Bureau of Administration, should identify the appropriate funding mechanisms and payment structures, if any, for SharePoint usage and share this information with SharePoint customers. (Action: IRM, in coordination with RM and A)

Recommendation 23: The Bureau of Information Resource Management, in coordination with the Bureaus of Resource Management, Administration, and Human Resources, should develop a transition plan for the Compensation Applications branch that includes, at a minimum, an assessment of skills and training needs for individuals and a determination of the post-transition role of the branch. (Action: IRM, in coordination with RM, A, and DGHR)

Recommendation 24: The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should determine what contractual arrangements are necessary to administer the payroll function pending its transition to the Bureau of Resource Management's portfolio and implement them accordingly. (Action: IRM, in coordination with A)

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 conduct periodic reviews of the Systems and Integration Office's mission and goals to measure its progress in meeting the Department of State's information technology strategic goals and make revisions as needed.

Informal Recommendation 2: The Bureau of Information Resource Management should label all servers and network devices at domestic data centers according to Department of State guidelines.

Informal Recommendation 3: The Bureau of Information Resource Management should mitigate the risk of water leakage from the pipes onto the server racks at Enterprise Service Operations Centers.

Principal Officials

	Name	Arrival Date
Director	Cynthia Cassil	Cynthia Cassil
Business Engagement Center	Catherine Walker	03/08
Collaboration and Compensation Services	Penny Duncan	07/09
Enterprise Programming and Integration	Michelle Sparrow-Walker	07/09
Enterprise Server Operations Center, Operations and Maintenance	C. Melonie Parker-Hill	06/07
Enterprise Server Operations Center, Design and Build	Raymond Brow	11/06

Abbreviations

BEC	Business Engagement Center division
CAPPS	Consolidated American Payroll Processing System
CCS	Collaboration and Compensation Services division
CEIS	Customer and Executive Information System
COR	Contracting officer's representative
D&B	Design and Build division
EPI	Enterprise Programming and Integration division
ESOC	Enterprise Server Operations Center
GTM	Government technical monitor
IRM	Bureau of Information Resource Management
IT	Information technology
ITSC	Information Technology Service Center
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance division
SDLC	Systems development lifecycle
SIO	Systems and Integration Office
SLA	Service level agreement

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

oig.state.gov

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