UNITED STATES CAPITOL POLICE
OFFICE OF INSPECTOR GENERAL

Independent Audit of USCP Enterprise Architecture

Report Number OIG-2012-01
December 2011

[redacted]

~~This report is intended solely for the official use of the United States Capitol Police or the Capitol Police Board, 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 United States Capitol Police or the Capitol Police Board, by them or by other agencies or organizations, without prior authorization by the Inspector General or the Capitol Police Board.~~

UNITED STATES CAPITOL POLICE
WASHINGTON, DC 20003

INSPECTOR GENERAL

PREFACE

The Office of Inspector General (OIG) prepared this report pursuant to the Inspector General Act of 1978, as amended. It is one of a series of audits, reviews, and investigative and special reports prepared by OIG periodically as part of its oversight responsibility with respect to the United States Capitol Police to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the office 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 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.

Carl W Hoecker
Carl W. Hoecker
Inspector General

TABLE OF CONTENTS

Appendices

Abbreviations

Capital Planning and Investment Control	CPIC
Chief Administrative Officer	CAO
Chief Information Officer	CIO
Chief Information Officer Council	CIOC
Control Objectives for Information and Related Technology	CobiT
Enterprise Architecture	EA
Enterprise Architecture Management Maturity Framework	EAMMF
Federal Enterprise Architecture Framework	FEAF
Fiscal Year	FY
Government Accountability Office	GAO
Information Technology	IT
Information Technology Governance Institute	ITGI
Investment Review Board	IRB
National Institute of Standards and Technology	NIST
Office of Financial Management	OFM
Office of Human Resources	OHR
Office of Information Systems	OIS
Office of Inspector General	OIG
Office of Management and Budget	OMB
Security Services Bureau	SSB
Special Publication	SP
The Practical Guide to Federal Enterprise Architecture	Practical Guide
Training Services Bureau	TSB
United States Capitol Police	USCP or the Department

EXECUTIVE SUMMARY

In accordance with our Fiscal Year (FY) 2011 annual plan, the Office of Inspector General (OIG) conducted a performance audit to determine whether the United States Capitol Police (USCP or Department) has (1) integrated its information technology (IT) strategy with the overall Department strategy and mission; (2) aligned IT resources and systems to support the Department's mission; (3) communicated and coordinated the business, mission-critical, and IT organizations within the Department; and (4) aligned IT investments in the budgeting and procurement processes. Our scope included Department information systems in production as of June 1, 2011.

We found that USCP has not integrated its IT strategy or aligned its IT resources and investments with the overall organization's strategy and mission or budget and procurement processes. The Department has not established (1) IT governance over Enterprise Architecture (EA) or (2) a repeatable business process to ensure that department-wide IT initiatives are aligned with the strategic direction of the Department. For example, the Office of Information Systems (OIS) strategic plan has not been updated since 2004, and OIS's *Catalog of Information Technology*, which provides an inventory of Department-wide information systems, was incomplete and did not reflect the "as is" configuration of the Department's technology. OIS cannot determine how their efforts and current technology support the mission and vision of USCP without a current strategic plan that identifies the OIS objectives and goals and an up-to-date inventory of systems in use by USCP.

Additionally, IT resources are decentralized within USCP, which has allowed redundant efforts and resources between offices and bureaus. As the main technology office, OIS provides the majority of the technology resources within the Department; however, "pockets" of technology exist throughout the organization. Office of Human Resources (OHR), Office of Financial Management (OFM), Training Services Bureau (TSB), and Security Services Bureau (SSB) include IT human resources that do not report to the Chief Information Officer (CIO). SSB also maintains an internal network of technology and systems independent from the technology supported by OIS. This lack of Department-wide policies, processes, and governance over IT resources (general expenses and personnel) contributes to inefficiencies and duplication of resources.

The Force Development Process is a process by which bureaus/offices map out their strategic initiatives and required resources for general expenses. For the last few years, however, the Department has not used the Force Development Process when making IT purchases, and bureaus and offices throughout the Department have independently procured IT software and systems without the input of the CIO or OIS. The procurement office also could not provide a detailed listing (purpose, cost, etc.) of Department-wide IT contracts and task orders, because the data was not retrievable without significant effort. As a result, bureaus and offices have purchased duplicative and competing software and systems, and at least one system has not been fully implemented, as shown below.

For example, OHR purchased a new [redacted] module for approximately $256,000 in February 2010 without receiving input from OIS or using the Force Development Process to review the purchase. At the time of purchase, OHR did not determine the full cost of the implementation, and according to the [redacted] vendor, it will cost an additional $600,000 to customize the module for the Department. OHR has not fully implemented the [redacted] module due to these unplanned costs. Additionally, through reviewing the list of Department systems in use compiled in Appendices C and D, systems appear to have been procured or developed internally to perform similar functions, including tracking, reporting, and record management. This occurred primarily because of a lack of alignment, via high priority segments, to agency strategic goals and objectives. The prioritization of IT through the procurement and budget process should be refined to reflect additional opportunities for cost savings and avoid redundancy to improve the Department's performance.

To develop an efficient and effective EA that supports the business processes and mission of USCP, OIG is recommending that the Department immediately establish governance over its IT endeavors to ensure that IT's performance is aligned with Department strategy and mission by exploiting opportunities and maximizing benefits, using resources responsibly, and managing related risks appropriately. Specifically, the Department should:

- Develop an EA policy and clearly define processes, roles, responsibilities, and authorities.
- Update the IT strategic plan and the Catalog of Information Technology.
- Consider integrating the Force Development Process with the IT review board for capital planning and investment control that links to budget formulation and execution.
- Evaluate the decentralized nature of the IT environment and consolidate redundant technology, systems, and utilization of IT support staff.

A complete listing of all OIG recommendations is shown in Appendix A.

On December 2, 2011, OIG conducted an exit conference with Department officials and provided a draft report for comment. We incorporated the Department's comments as applicable and attached their response to the report in its entirety in Appendix B.

BACKGROUND

USCP is the law enforcement agency within the legislative branch of the U.S Government that is tasked with protecting the Capitol Complex and the members of the United States Congress, both domestically and abroad. In support of the Department's mission, USCP has [redacted] IT systems[2] to conduct USCP's business through its bureaus and offices. USCP's technology office, OIS,

[redacted]

[2] The term "information system" used in this report is based on the definition provided by OMB Circular A-130: "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

provides enterprise-wide IT solutions and supports a wide range of systems in use. In addition to the technology solutions provided by OIS, other bureaus and offices operate and maintain technology without support and consultation from OIS. In FY 2011, USCP's budget included nearly $14 million dollars for OIS. This figure does not represent the monies budgeted for the radio modernization project or the other bureaus and offices' technology investment.

In FY 2007, the Department created the Force Development Process, which is designed to link business planning to budget planning so that resource initiatives can be analyzed and prioritized from a Department-wide focus. The Force Development Process is completed annually in preparation for the Department's annual budget submission.

EA is a blueprint that describes both the current and desired state of an organization or functional area in both logical and technical terms, as well as a plan for transitioning between the two states. Without EA, it is unlikely that an organization could transform business processes and modernize supporting systems to minimize overlap and maximize interoperability. Moreover, legislation and federal guidance requires agencies to develop and use architectures.

As a legislative branch entity, many laws and regulations that apply to executive branch agencies do not apply to USCP; however, we believe these laws and regulations represent appropriate guidance and industry best practices for USCP. Congress enacted the Information Technology Management Reform Act of 1996 (known as the Clinger-Cohen Act[3]) to improve the management of agencies' information systems. The Clinger-Cohen Act requires the head of each federal agency to implement processes for maximizing the value and assessing and managing the risks of executive agencies' information technology acquisitions by:

- Focusing information resource planning to support their strategic missions.
- Implementing a capital planning and investment control process that links to budget formulation and execution.
- Rethinking and restructuring the way they do their work before investing in information systems.

Clinger-Cohen also requires the CIO of each agency to develop, maintain, and facilitate the implementation of IT architectures as a means of integrating business and operational processes to support the agency's mission and goals.

Office of Management and Budget (OMB) Circular A-130 (A-130)[4] contains policy framework for the management of Federal information resources. Originally released in 1985, OMB A-130 has been revised to incorporate various laws and regulations, including the Clinger-Cohen Act. The circular provides guidance and requirements for many aspects of IT, including EA and capital planning and investment control (CPIC) processes. The Chief Information Officer Council's (CIOC) *Architecture Alignment and Assessment Guide* (2000) refers to OMB A-130 as the "one-stop shopping document for OMB policy and guidance on information technology management." OMB A-130 emphasizes that IT and investment in IT must align to the agency's mission while effectively and efficiently supporting the strategic vision of the agency.

[3] Pub. L. 104-106, Division E.
[4] Transmittal Memorandum #4, Management of Federal Information Resources (11/28/2000).

Various frameworks have been developed to assist agencies with implementing an EA program, including the *Federal Enterprise Architecture Framework* (FEAF). CIOC published the *Practical Guide to Federal Enterprise Architecture* (Practical Guide) in 2001 in support of this framework. The Practical Guide describes EA as a strategic information asset base that defines the mission, the information and technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs.

EA includes baseline architecture, target architecture, and a sequencing plan. EA is comprised of four elements: Business Architecture, Data Architecture, Applications Architecture, and Technology Architecture. Together, these elements provide a clear picture of how an organization accomplishes its mission, goals, and objectives. Each of the four architectures is comprised of a current or "as-is" element that describes the existing environment, a target or "to-be" element that describes the proposed environment, and a sequencing plan detailing the transition from the "as-is" to the "to-be" environment.

Enterprise Architecture Management Maturity Framework[5] (EAMMF) was developed by the Government Accountability Office (GAO) in 2003, in collaboration with OMB and CIOC. The GAO EA framework consists of three basic components: (1) hierarchical *stages* of management maturity, (2) categories of *attributes* that are critical to success in managing any endeavor, and (3) *elements* of EA management that form the core of the Practical Guide. Elements referred to as "core elements" are descriptions of a practice or condition that is needed for effective EA management. The EAMMF defines 31 core elements that are derived from the Practical Guide. See Appendix E for detailed descriptions of the five maturity stages, critical success attributes, core elements, and a depiction of their interrelationships.

OBJECTIVE, SCOPE, AND METHODOLOGY

On behalf of the OIG, Cotton & Company LLP conducted an independent performance audit of the Department's EA program to determine whether the following has been achieved:

- Integration of the IT strategy with the overall Department strategy and mission.
- Alignment of IT resources and systems to support the Department's mission.
- Communication and coordination among the business, mission-critical, and IT organizations within USCP.
- Alignment of IT investments in the budgeting and procurement processes.

Our scope included Department information systems in production as of June 1, 2011.

[5] *Information Technology, A Framework for Assessing and Improving Enterprise Architecture Management*, Version 1.1 (GAO-03-584G), dated April 2003

To accomplish these objectives, we first interviewed CIO and OIS staff to gain an understanding of the:

- Current OIS structure and strategy, and how OIS supports the USCP mission.
- Current EA efforts underway.
- EA policies and procedures.
- Resources dedicated to EA.
- Budgeting process and OIS's involvement in the Force Development Process.

Based on these meetings, we conducted additional interviews with Office Directors aligned under the Chief Administrative Officer (CAO) and the Bureau Commanders aligned under the Assistant Chief of Police (ACOP). Offices under the CAO provide USCP with the necessary administrative functions to support its mission, including Human Resources, Financial Management, Logistics, Training, and Policy. Bureaus under the ACOP are the operational law enforcement resources that accomplish the USCP mission, including Mission Assurance, Operational Services, Protective Services, Security Services, and Uniformed Services.

In addition, we reviewed documentation on the OIS organizational structure, inventories of systems maintained by OIS, inventories of systems used by each bureau/office, Department and office budgets, relevant policies and procedures, executive committee charters, and documentation created as part of the Force Development process.

We used guidance from OMB, National Institute of Standards and Technology (NIST), GAO, and CIOC to determine the industry best practices for implementing EA. Using the assessment framework established by GAO through its EAMMF, we assessed the Department's efforts to implement an EA program at Maturity Stage 1: *Creating Enterprise Architecture Awareness.*

We conducted this performance audit in Washington, D.C. from June through October 2011, in accordance with generally accepted government auditing standards, and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management officials on December 2, 2011, and included their comments where appropriate. We did not audit the Department's responses, and accordingly, we express no opinion on them.

RESULTS

USCP has not integrated its IT strategy or aligned its IT resources and investments with the overall organization's strategy and mission or budget and procurement processes. The Department also has not established an EA management foundation (governance) or developed a repeatable business process to ensure that department-wide IT initiatives are aligned with the strategic direction of the Department. Additionally, IT resources are decentralized within USCP, and the Department has not used its Force Development Process for capital planning and investment, which has allowed redundant efforts and resources to exist between offices and bureaus.

INADEQUATE INTEGRATION OF INFORMATION TECHNOLOGY

USCP has not integrated its IT strategy with the overall Department strategy and mission. According to Policenet, OIS is responsible for providing policy, as well as planning, budgeting, designing, testing, implementing, and managing the Department's automated information and information technologies. We found that the *OIS Strategic Plan* is outdated, however, and does not align with the overall *USCP Strategic Plan*. OIS has not updated its strategic plan since 2004. According to the OIS Director, OIS does not have resources fully dedicated to the EA effort and has shifted focus away from creating and maintaining the documents and policies that provide the foundation of the EA effort. OIS cannot determine how their efforts and current technology support the mission and vision of USCP without a current strategic plan that identifies the OIS objectives and goals. OMB Circular Number (No.) 130, *Management of Federal Information Resources,* states:

> *In the capital planning and investment control process, there are two separate and distinct plans that address IRM and IT planning requirements for the agency. The IRM Strategic Plan is strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency Information Resource Management Strategic Plan (IRM) as required by 44 U.S.C. 3506 (b) (2). IRM Strategic Plans should support the agency Strategic Plan required in OMB Circular A-11, provide a description of how information resources management activities help accomplish agency missions, and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.*

IT Governance Institute (ITGI) *Control Objectives for Information and related Technology (CobiT)*, version 4.1, *PO1 Define a Strategic IT Plan*, states:

> *IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realized from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource requirements, and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.*

CIOC, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 dated February 2001, states:

> *...The process of getting the enterprise from where it is today to where it wants to be in the future needs formal thought and that focuses on optimizing enterprise-wide performance and accountability. This thought process is documented with the Agency's strategic plan. This document defines the mission and long-range objectives of the Agency and relates to plans for business reengineering and systems modernization. Together these products should drive the topdown sequence of EA product development...*

Conclusions

IT strategic planning is required to manage and direct all IT resources to optimize support of the business strategy and priorities. The *OIS Strategic Plan* is outdated, however, and does not align with the overall *USCP Strategic Plan*. As a result, OIS cannot determine how their efforts and current technology supports the mission and vision of the Department. Thus, OIG is making the following recommendation.

> **Recommendation 1: We recommend the United States Capitol Police, Office of Information Systems, immediately update its strategic plan to define objectives and goals that align with the short- and long-term goals and objectives of the Department. This plan also should incorporate goals on optimizing enterprise-wide information systems performance and accountability.**

LACK OF GOVERNANCE OVER ENTERPRISE ARCHITECTURE

Although the Department is not subject to many of the laws and regulations that apply to the executive branch, we believe these regulations provide industry best practices. GAO's framework provides a roadmap to establishing and leveraging architectures for organizational transformation. The framework's core elements can be placed in one of four groups of architecture-related activities, processes, products, events, and structures. These groups are architecture governance, content, use, and measurement. Our assessment showed that the Department lacks governance over EA. Specifically, the Department has not achieved 11 of 12 core elements of the governance group evaluated during this audit, as shown in Table 1.

TABLE 1: GOVERNANCE GROUP CORE ELEMENTS

Governance Group Core Elements	*Not Achieved*
Adequate resources exist (stage 2).	Did not evaluate.
Committee or group representing the enterprise is responsible for directing, overseeing, and approving EA (stage 2).	☑
Program office responsible for EA development and maintenance exists (stage 2).	OIS
Chief architect exists (stage 2).	☑
EA being developed using a framework, methodology, and automated tool (stage 2).	☑
EA plans call for describing "as-is" environment, "to-be" environment, and sequencing plan (stage 2).	☑
EA plans call for describing enterprise in terms of business, performance, information/data, application/service, and technology (stage 2).	☑
EA plans call for business, performance, information/data, application/service, and technology to address security (stage 2).	☑
Written and approved policy exists for EA development (stage 3).	☑
Organization CIO has approved EA (stage 4).	☑
Committee or group representing the enterprise or the investment review board has approved current version of EA (stage 4).	☑
Written and approved organization policy exists for IT investment compliance with EA (stage 5).	☑
Organization head has approved current version of EA (stage 5).	☑

Oversight Committee Not Established and Chief Architect Not Identified

The Department has not established a committee or group responsible for overseeing EA or identified a Chief Architect. GAO, *A Framework for Assessing and Improving Enterprise Architecture Management*, Version 1.1, states:

> *...An organization should assign responsibility for directing, overseeing, and approving the architecture not to just one individual, but to a committee or group with representation from across the enterprise. Establishing this enterprise wide responsibility and accountability is important in demonstrating the organization's commitment to building the management foundation and obtaining buy-in from across the organization. Accordingly, this group should include executive-level representatives from each line of business, and these representatives should have the authority to commit resources and enforce decisions within their respective organizational units. Typically, this group, established by the organization head, serves as a "steering committee" and is responsible for guiding, directing, and approving EA plans and products, including significant changes to either...*

Additionally, CIOC, *A Practical Guide to Federal Enterprise Architecture,* Version 1.0, Section 3.2.4 states:

> *The CIO should appoint, with the Agency Head's approval, an Agency executive to serve as Chief Architect and EA Program Manager. The Chief Architect is responsible for leading the development of the EA work products and support environment. The Chief Architect serves as the technology and business leader for the development organization, ensuring the integrity of the architectural development processes and the content of the EA products. The Chief Architect should be friend and liaison to the business line units and ensure that business unit processes are emphasized in the EA. Likewise; the Chief Architect is responsible for ensuring that the EA provides the best possible information and guidance to IT projects and stakeholders, and that systems development efforts are properly aligned with business unit requirements.*

Enterprise Architecture Policy Not Developed or Implemented

The Department has not developed a formal policy that governs the development, implementation, and maintenance of EA for USCP. OIS has not dedicated resources to support the EA initiative, including developing and maintaining appropriate documentation. Without a formalized policy that governs the development and implementation of the EA plan, it will be difficult to implement a robust program that will effectively align OIS's projects, programs, and infrastructure to fully support the USCP mission and vision. CIOC, *A Practical Guide to Federal Enterprise Architecture,* Version 1.0 states:

> *The CIO, in collaboration with the Agency Head, develops a policy based on the Agency's architecture principles that governs the development, implementation, and maintenance of the EA. The EA policy should be approved by the Agency Head and, at a minimum, should include:*
>
> - *Description of the purpose and value of an EA*
> - *Description of the relationship of the EA to the Agency's strategic vision and plans*
> - *Description of the relationship of the EA to capital planning, enterprise engineering, and program management*
> - *Translation of business strategies into EA goals, objectives, and strategies*

- *Commitment to develop, implement, and maintain an EA*
- *Identification of EA compliance as one criterion for new and ongoing investments*
- *Overview of an enforcement policy*
- *Security practices to include certification and accreditation*
- *Appointment of the Chief Architect and establishment of an EA core team*

Enterprise Architecture Review Board

The Department has not established, documented, and implemented an EA Review Board, IT Steering Committee, or similar group to assess the current state of the enterprise and evaluate new initiatives. During the annual Force Development Process, the Executive Management Team and Executive Team have not selected these EA program initiatives to be included in either the FY 2012 or FY 2013 budget submissions for USCP. Without effective oversight from the EA Review Board on current and new initiatives, USCP and OIS cannot effectively determine whether technology, either currently in use or planned, will effectively support USCP's mission and vision.

Additionally, OHR purchased a new [redacted] module for approximately $256,000 in February 2010 without receiving input from OIS or using the Force Development Process to review the purchase. At the time of purchase, OHR did not determine the full cost of the implementation, and according to the [redacted] vendor, it will cost an additional $600,000 to customize the module for the Department. OHR has not fully implemented the [redacted] module due to these unplanned costs. Thus, without a review board, the Force Development Process will not accurately capture the full cost of implementing a system at USCP. CIOC, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0, states:

> *…The CIO should charter and appoint a Technical Review Committee (TRC) to manage the review of candidate projects and assess project alignment with the EA. Once the EA has been developed and approved, the TRC assesses each proposed investment for compliance with the architecture…*

OMB Memorandum M-11-29: Chief Information Officer Authorities, dated August 8, 2011, also states:

> 1. *Governance. CIOs must drive the investment review process for IT investments and have responsibility over the entire IT portfolio for an Agency. CIOs must work with Chief Financial Officers and Chief Acquisition Officers to ensure IT portfolio analysis is an integral part of the yearly budget process for an agency…*

Conclusions

USCP is generally aware of EA but has yet to implement a sustainable architecture that will facilitate the integration of IT with the Department's strategy to support its mission. IT currently does not have adequate governance to properly align IT resources throughout the Department. Specifically, the Department has not established a committee, group, or chief architect responsible for directing, overseeing, and approving EA. The Department neither developed and implemented an EA policy nor established an EA Review Board to assess the current state of the enterprise. Thus, OIG is making the following recommendation.

Recommendation 2: We recommend the United States Capitol Police implement the core elements of the Government Accountability Office's enterprise architecture Governance group, to include establishing an oversight committee and review board; identifying a Chief Architect; and developing a formal policy that governs the development, implementation, and maintenance of enterprise architecture for the Department.

DECENTRALIZED INFORMATION TECHNOLOGY RESOURCES

IT resources are decentralized within the Department, which has allowed redundant efforts and resources to exist between offices and bureaus. OIS provides the majority of the technology resources within the Department; however, "pockets" of technology exist throughout the organization. OHR, OFM, TSB, and SSB include IT human resources that do not report to the CIO, as shown in Table 2. SSB also maintains an internal network of technology and systems independent from the technology supported by OIS.

TABLE 2: POCKETS OF INFORMATION TECHNOLOGY RESOURCES

Department Bureau or Office	*Number of Resources*	*Function*
Office of Financial Management (OFM)	3 Department employees	System and Security Administrators for the Department's financial systems.
Office of Human Resources (OHR)	1 Department employee	System, Security, and Database Administrator for the Department's human resource systems.
Training Services Bureau (TSB)	1 Department employee	Technical support to the Department's training facility located in Maryland. The TSB resource maintains and supports systems used by TSB.
Office of Information Systems (OIS)	22 Department employees	Provides support for OIS operations, including communications, IT help desk, security, network operations, and software development.
	32 Contractors	
Security Services Bureau (SSB)	6 Department employees	Provides support to SSB's internal network, both infrastructure and software. Additionally, support data entry and daily operations of SSB systems.
	30 Contractors[6]	Provides support to SSB's technology. SSB Contractors are cross-trained on the majority of SSB technology.

Source: Compiled based on discussions with bureaus and offices.

The Department created the Force Development Process in FY 2007. This process is designed to link business planning to budget planning so that resource initiatives can be analyzed and prioritized from a Department-wide focus. During the FY 2010 and FY 2011 budget formulation process, the Department did not use the Force Development Process for IT purchases. This lack of

[6] Number of contractors supporting SSB as of July 21, 2011 interview. Number of contractors reduced to 24 during the reporting period of audit.

Department-wide policies, processes, and governance over IT resources (general expenses and personnel) has contributed to inefficiencies and contributed to an incomplete inventory of IT systems.

Because the IT function does not fully report to the CIO, over the years bureaus and offices throughout USCP have developed or procured systems without involvement from OIS. These systems are not communicated to OIS for inclusion in the catalog. As a result, OIS's *Catalog of Information Systems* does not completely or accurately reflect the current systems across the USCP enterprise, and senior Department leadership does not have a complete list of IT resources. An effort by a contractor to update the catalog was underway early in 2011; however, as of our audit period this effort was halted due to the cancelation of the contract.

One of the underlying principles of EA is to define the "as is" and "to be" configurations. Without an up-to-date inventory of systems in use by USCP, OIS is unable to identify its current "as is" configuration. As a result, OIS would not be able to completely and accurately define its transition plans to the "to be" configuration. Through this audit, we compiled a listing of IT systems identified by Department officials, as shown in Appendix C. NIST Special Publication (SP) 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, Version 1.0, states:

> *... the creation of a system inventory to ensure the agency can identify CBSR and investment ownership information and review investment performance accordingly. The system inventory is a cornerstone of the ITIM framework and also relates directly to investment security concerns. Both FISMA and the ITIM framework require the development of a system inventory. FISMA requires the inventory to identify the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency. The FISMA requirement stems from OMB's expectation that each agency have such an inventory in accordance with its work on developing its Enterprise Architecture. FISMA also requires that the inventory be updated at least annually. Agencies should work to build a single system inventory that meets the requirements of both the ITIM framework and FISMA...*

OIS and SSB utilize the largest number of IT resources and maintain independent networks of technology and systems. Without communication and coordination, there is an increased risk of redundant efforts and resources between these areas. This may cause inefficiencies for USCP, including but not limited to procurement of IT assets and the development, operation, and maintenance of technology. To an extent, similar resources are required to develop, operate, and maintain technology infrastructures regardless of the sensitivity level of that infrastructure. Additionally, in an environment with decentralized IT resources that are not aligned to the technology office, there is an increased risk that these resources will provide customer support that is inconsistent with the approved methodologies communicated from the technology office. Finally, with a decentralized IT support environment, it is difficult to understand the business needs of the entire organization and determine an effective transition schedule as part of the EA program. OMB Memorandum M-11-29: *Chief Information Officer Authorities*, dated August 8, 2011, states:

> *1. Governance. CIOs must drive the investment review process for IT investments and have responsibility over the entire IT portfolio for an Agency..."*

> *2. Commodity IT. Agency CIOs must focus on eliminating duplication and rationalize their agency's IT investments. Agency commodity services are often duplicative and sub-scale and include services such as: IT infrastructure (data centers, networks, desktop computers and mobile devices); enterprise IT systems (e-mail, collaboration tools, identity and access management, security, and web infrastructure); and business systems (finance, human resources, and other administrative functions). The CIO shall pool their agency's purchasing power across their entire organization to drive down costs and improve service for commodity IT. In addition, enterprise architects will support the CIO in the alignment of IT resources, to consolidate duplicative investments and applications…*

OMB *Enterprise Architecture Assessment Framework*, version 3.1, Section 2.2 Invest, also states:

> *During this step of the Performance Improvement Lifecycle, agencies should carefully evaluate and adjust their prioritization to ensure investments are aligned, via high priority segments, to agency strategic goals and objectives. Further, the prioritization should be refined to reflect additional opportunities for cost savings and avoidance, as well as other approaches to improve agency performance...*

Conclusions

IT resources are decentralized within the Department, which has allowed redundant efforts and resources to exist between offices and bureaus. Additionally, a lack of Department-wide policies, processes, and governance over IT resources (general expenses and personnel) has contributed to inefficiencies and resulted in an incomplete inventory of IT systems. Although the Department has a review process for new initiatives and programs to ensure that existing threats perceived by USCP are mitigated, IT purchase(s) have not been reviewed through this process in recent years. Thus, OIG is making the following recommendations.

> **Recommendation 3: We recommend the United States Capitol Police management evaluate the distinct organizations with significant information technology investments and operations. As part of this evaluation, all individuals within the organization, either within Office of Information Systems or other bureaus and offices that have any information technology support responsibilities, should be identified. Once identified, an analysis should be performed to determine how those individuals can be aligned within Office of Information Systems. If re-alignment is not feasible, the individuals' information technology responsibilities should be transitioned to appropriate individuals within Office of Information Systems. Furthermore, as part of the evaluation, duplicate technology infrastructure, i.e., datacenters, should be identified and consolidated.**

> **Recommendation 4: We recommend the United States Capitol Police immediately complete a full inventory of systems in use by the Department to identify its "as is" configuration. Once developed and validated, Office of Information Systems should develop the Department's "to be" configuration and its transition plan to achieve this configuration.**

Recommendation 5: We recommend that the United States Capitol Police Enterprise Architecture Review Board's decisions and recommendations be incorporated into the decision-making process that aligns its information technology investments with the budgeting and procurement processes (Force Development Process).

APPENDICES

Listing of Recommendations

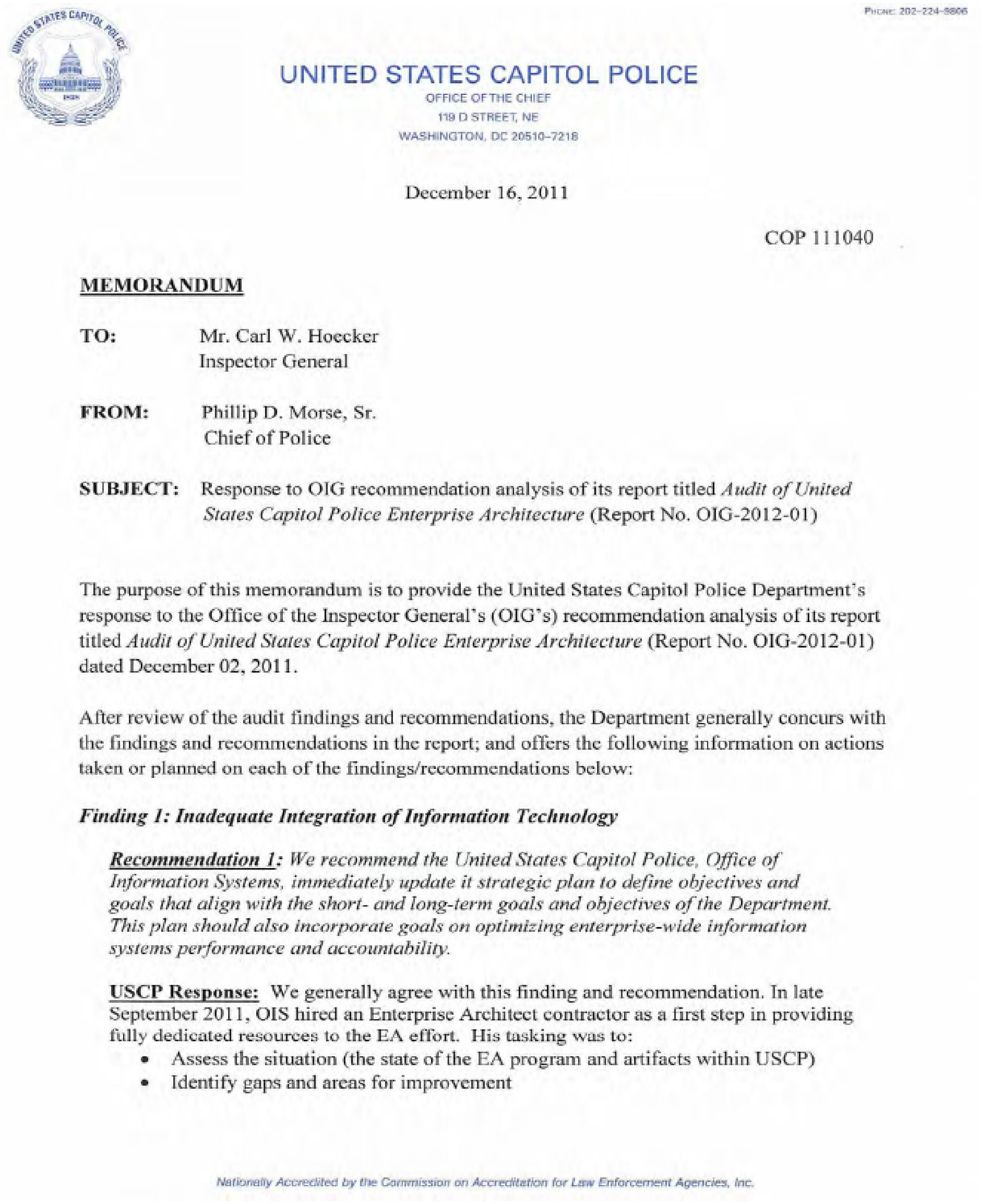
Recommendation 1: We recommend the United States Capitol Police, Office of Information Systems, immediately update its strategic plan to define objectives and goals that align with the short- and long-term goals and objectives of the Department. This plan also should incorporate goals on optimizing enterprise-wide information systems performance and accountability.

Recommendation 2: We recommend the United States Capitol Police implement the core elements of the Government Accountability Office's enterprise architecture Governance group, to include establishing an oversight committee and review board; identifying a Chief Architect; and developing a formal policy that governs the development, implementation, and maintenance of enterprise architecture for the Department.

Recommendation 3: We recommend the United States Capitol Police management evaluate the distinct organizations with significant information technology investments and operations. As part of this evaluation, all individuals within the organization, either within Office of Information Systems or other bureaus and offices that have any information technology support responsibilities, should be identified. Once identified, an analysis should be performed to determine how those individuals can be aligned within Office of Information Systems. If re-alignment is not feasible, the individuals' information technology responsibilities should be transitioned to appropriate individuals within Office of Information Systems. Furthermore, as part of the evaluation, duplicate technology infrastructure, i.e., datacenters, should be identified and consolidated.

Recommendation 4: We recommend the United States Capitol Police immediately complete a full inventory of systems in use by the Department to identify its "as is" configuration. Once developed and validated, Office of Information Systems should develop the Department's "to be" configuration and its transition plan to achieve this configuration.

Recommendation 5: We recommend that the United States Capitol Police Enterprise Architecture Review Board's decisions and recommendations be incorporated into the decision-making process that aligns its information technology investments with the budgeting and procurement processes (Force Development Process).



PHONE: 202-224-9806

UNITED STATES CAPITOL POLICE
OFFICE OF THE CHIEF
119 D STREET, NE
WASHINGTON, DC 20510-7218

December 16, 2011

COP 111040

MEMORANDUM

TO: Mr. Carl W. Hoecker
Inspector General

FROM: Phillip D. Morse, Sr.
Chief of Police

SUBJECT: Response to OIG recommendation analysis of its report titled *Audit of United States Capitol Police Enterprise Architecture* (Report No. OIG-2012-01)

The purpose of this memorandum is to provide the United States Capitol Police Department's response to the Office of the Inspector General's (OIG's) recommendation analysis of its report titled *Audit of United States Capitol Police Enterprise Architecture* (Report No. OIG-2012-01) dated December 02, 2011.

After review of the audit findings and recommendations, the Department generally concurs with the findings and recommendations in the report; and offers the following information on actions taken or planned on each of the findings/recommendations below:

Finding 1: Inadequate Integration of Information Technology

Recommendation 1: *We recommend the United States Capitol Police, Office of Information Systems, immediately update it strategic plan to define objectives and goals that align with the short- and long-term goals and objectives of the Department. This plan should also incorporate goals on optimizing enterprise-wide information systems performance and accountability.*

USCP Response: We generally agree with this finding and recommendation. In late September 2011, OIS hired an Enterprise Architect contractor as a first step in providing fully dedicated resources to the EA effort. His tasking was to:

- Assess the situation (the state of the EA program and artifacts within USCP)
- Identify gaps and areas for improvement

Nationally Accredited by the Commission on Accreditation for Law Enforcement Agencies, Inc.

- Develop an EA Plan of Action
- Execute the plan

The results of this audit fully support/complement the results from the first two taskings above, and the audit recommendations will be fully integrated in the EA Plan of Action currently being developed. An EA Task Force will be constituted to provide the resources to accomplish the various action items within the plan. The EA Task Force will be subdivided into teams to address the following areas:

- Information Technology Strategic Plan
- EA Governance
- IT Capitol Planning Investment Control (CPIC) integration with the Force Development process
- Catalog of IT ("as-is" and "to-be")
- Consider centralization of USCP IT

Drafting a new Information Technology Strategic Plan that is aligned with the USCP Strategic Plan for FY 2011-2015 will be one of the first actions listed in the plan. We will include in the Information Technology Strategic Plan, as objectives, actions resulting from this audit such as increasing the EA Maturity stage level for the Department. Over the past several months, OIS has been working on a Program Work Breakdown Structure that aligns with the USCP Strategic Plan. This artifact will be shared and aggregated with other outputs the EA Task Force Teams produce.

Finding 2: Lack of Governance over Enterprise Architecture

<u>Recommendation 2</u>: *We recommend the United States Capitol Police implement the core elements of the Government Accountability Office's enterprise architecture Governance group, to include establishing an oversight committee and review board; identifying a Chief Architect; and developing a formal policy that governs the development, implementation, and maintenance of enterprise architecture for the Department.*

<u>USCP Response:</u> We generally agree with this finding and recommendation. OIS will take the lead in developing a formal EA policy and establishing an Oversight Committee and Review Board. These actions will fall under the EA Governance team mentioned above. With the Executive Team's approval, the CIO will appoint a Chief Architect from existing personnel. Should budget constraints ease and allow for an FTE position for a Chief Architect, the position will be prioritized within the existing civilian hiring process. The Department will accept the goal of increasing the Department's EA Maturity stage level by implementing the core elements of the GAO's EA Governance group.

Finding 3: Decentralized Information Technology Resources

<u>Recommendation 3</u>: *We recommend the United States Capitol Police management evaluate the distinct organizations with significant information* *technology investments and operations. As part of this evaluation, all individuals within the organization, either within the Office of Information Systems or other bureaus and offices that have any information technology support responsibilities, should be identified. Once identified, an analysis should be performed to determine how those individuals can be aligned within the Office of Information Systems. If re-alignment is not feasible, the individuals' information technology responsibilities should be transitioned to the appropriate individuals within the Office of Information Systems. Furthermore, as part of the evaluation, duplicate technology infrastructure, i.e., datacenters, should be identified and consolidated.*

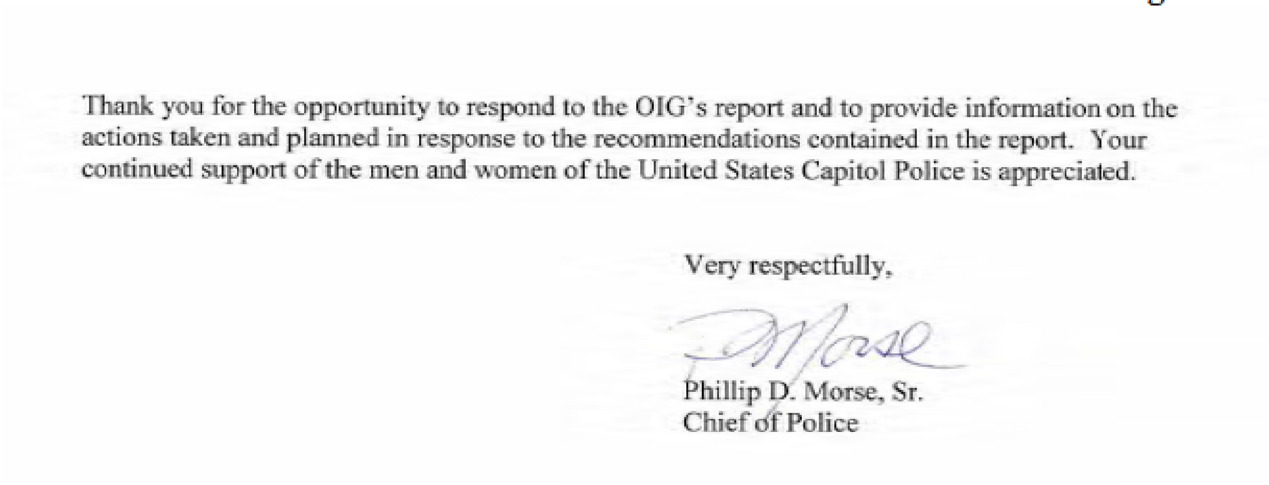
USCP Response: The Department will review each situation of decentralized information technology (IT) and the EA task force will develop recommendations based on the overall "inventory" of IT assets for the Executive Team's consideration and decision. These recommendations will be based on the core mission requirements for the Department, our obligations related to Title 50 equivalence or other national security agreements, the specific requirements of the Legislative Branch, and the best practices proposed by the Government Accountability Office.

Recommendation 4: *We recommend the United States Capitol Police immediately complete a full inventory of systems in use by the Department to identify its "as is" configuration. Once developed and validated, Office of Information Systems should develop the Department's "to be" configuration and its transition plan to achieve this configuration.*

USCP Response: We generally agree with this recommendation. The Catalog of IT team has been working on updating the "as-is" section of the catalog for the past two months. The initial focus was on updating OIS systems and recently the team has started bi-weekly collaborative meetings with selected Subject Matter Experts throughout USCP in an effort to increase the utility of the existing IT catalog and refine the current "as-is" EA state. These engineering artifacts will be used to optimize future technology implementations, as well as help establish a direction and path forward for USCP's "to-be" Enterprise Architecture.

Recommendation 5: *We recommend that the United States Capitol Police Enterprise Architecture Review Board's decisions and recommendations be incorporated into the decision-making process that aligns its information technology investments with the budgeting and procurement processes (Force Development Process).*

USCP Response: We generally agree with this recommendation. The IT CPIC integration with the Force Development team mentioned above will take this recommendation for action. They will develop, in collaboration with the EA Governance team and OPOL, a proposed IT CPIC process that aligns and integrates with the Force Development process. The proposed process will be submitted to the ET for consideration and approval.



Thank you for the opportunity to respond to the OIG's report and to provide information on the actions taken and planned in response to the recommendations contained in the report. Your continued support of the men and women of the United States Capitol Police is appreciated.

Very respectfully,

PMorse

Phillip D. Morse, Sr.
Chief of Police

Listing of Sensitive USCP Systems

Through inquiries with Bureau Commanders and the listings created by each office and bureau as requested during the audit period, we noted that the Department uses a number of law enforcement sensitive systems. These other [redacted] systems are considered security information as defined by United States Code[7] and the Legislative Branch Appropriations Act of 2005[8]. As such, these systems have been included in the Department system counts noted in this report; however, they have not been listed in detail in accordance with this law. This listing is maintained by the OIG.

[7] 2 U.S.C. § 1979

[8] Pub. L. 108-447, Division. G, Title I, Section. 1009

Summary of Enterprise Architecture Management Framework's Maturity Stages, Critical Success Attributes, and Core Elements

The five maturity stages of the EAMMF:

Stage 1: Creating Enterprise Architecture Awareness
At Stage 1, either an organization does not have plans to develop and use an architecture, or it has plans that do not demonstrate an awareness of the value of having and using an architecture. While Stage 1 agencies may have initiated some EA activity, these agencies' efforts are ad hoc and unstructured, lack institutional leadership and direction, and do not provide the management foundation necessary for successful EA development as defined in Stage 2.

Stage 2: Building the Enterprise Architecture Management Foundation
An organization at Stage 2 recognizes that the EA is a corporate asset by vesting accountability for it in an executive body that represents the entire enterprise. At this stage, an organization assigns EA management roles and responsibilities and establishes plans for developing EA products and for measuring program progress and product quality; it also commits the resources necessary for developing an architecture.

Stage 3: Developing the Enterprise Architecture
An organization at Stage 3 focuses on developing architecture products according to the selected framework, methodology, tool, and established management plans. Roles and responsibilities assigned in the previous stage are in place, and resources are being applied to develop actual EA products. Here, the scope of the architecture has been defined to encompass the entire enterprise, whether organization-based or function-based. Further, the products are to describe the current ("as-is") and future ("to-be") states and the plan for transitioning from the current to the future state (the sequencing plan).

Stage 4: Completing the Enterprise Architecture
An organization at Stage 4 has completed its EA products, meaning that the products have been approved by the EA steering committee (established in Stage 2) or an investment review board, and by the CIO. The completed products collectively describe the enterprise in terms of business, performance, information/data, service/application, and technology for both its current and future operating states, and the products include a transition plan for sequencing from the current to the future state.

Stage 5: Leveraging the Enterprise Architecture to Manage Change
An organization at Stage 5 has secured senior leadership approval of the EA products and a written institutional policy stating that IT investments must comply with the architecture, unless granted an explicit compliance waiver. Further, decision-makers are using the architecture to identify and address ongoing and proposed IT investments that are conflicting, overlapping, not strategically linked, or redundant.

With the exception of the first stage, each maturity stage is composed of the following four success attributes that are critical to the successful performance of any management function:

Attribute 1: Demonstrates Commitment
Support from the head of the enterprise is essential to the success of the architecture effort. An approved enterprise policy statement provides such support and sponsorship, promoting institutional "buy-in" and encouraging resource commitment from participating components.

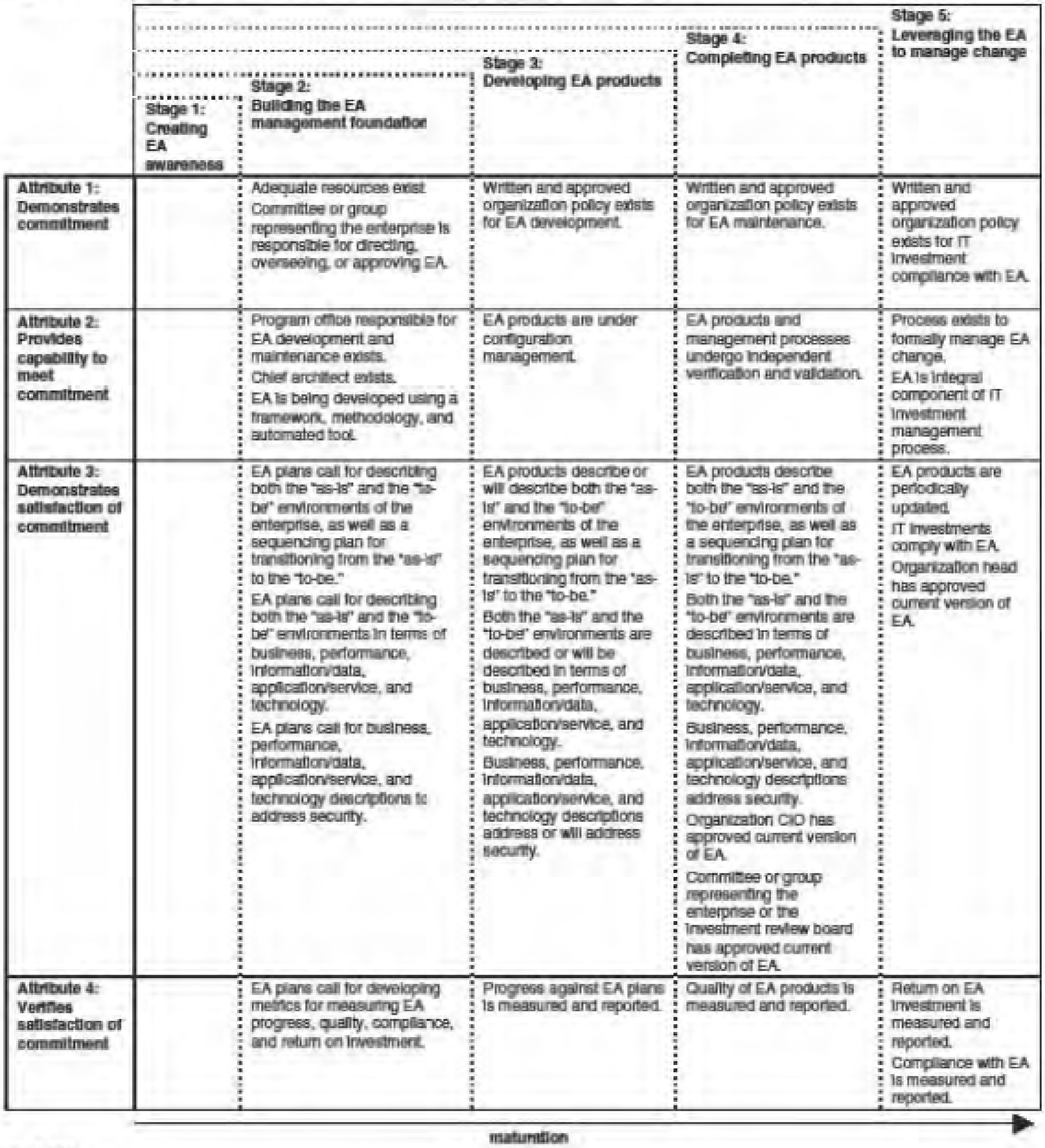
Attribute 2: Provides Capability to Meet Commitment
The success of the EA effort depends largely on the organization's capacity to develop, maintain, and implement the EA. Consistent with any large IT project, these capabilities include providing adequate resources, i.e., people, processes, and technology; defining clear roles and responsibilities; and defining and implementing organizational structures and process management controls that promote accountability and effective project execution.

Attribute 3: Demonstrates Satisfaction of Commitment
Demonstrating satisfaction of the organization's commitment to develop, maintain, and implement an EA is evidenced by the production of artifacts, e.g., the plans and products.

Attribute 4: Verifies Satisfaction of Commitment
This attribute focuses on measuring and disclosing the extent to which efforts to develop, maintain, and implement the EA have fulfilled stated goals or commitments.

Each attribute contains core elements that contribute to the successful implementation that attribute. The matrix below, developed by GAO, depicts the interconnections between maturity stages, attributes, and core elements.

Figure 6: Summary of EAMMF Version 1.1: Maturity Stages, Critical Success Attributes, and Core Elements



	Stage 1: Creating EA awareness	Stage 2: Building the EA management foundation	Stage 3: Developing EA products	Stage 4: Completing EA products	Stage 5: Leveraging the EA to manage change
Attribute 1: Demonstrates commitment		Adequate resources exist. Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA.	Written and approved organization policy exists for EA development.	Written and approved organization policy exists for EA maintenance.	Written and approved organization policy exists for IT investment compliance with EA.
Attribute 2: Provides capability to meet commitment		Program office responsible for EA development and maintenance exists. Chief architect exists. EA is being developed using a framework, methodology, and automated tool.	EA products are under configuration management.	EA products and management processes undergo independent verification and validation.	Process exists to formally manage EA change. EA is integral component of IT investment management process.
Attribute 3: Demonstrates satisfaction of commitment		EA plans call for describing both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be." EA plans call for describing both the "as-is" and the "to-be" environments in terms of business, performance, information/data, application/service, and technology. EA plans call for business, performance, information/data, application/service, and technology descriptions to address security.	EA products describe or will describe both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be." Both the "as-is" and the "to-be" environments are described or will be described in terms of business, performance, information/data, application/service, and technology. Business, performance, information/data, application/service, and technology descriptions address or will address security.	EA products describe both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be." Both the "as-is" and the "to-be" environments are described in terms of business, performance, information/data, application/service, and technology. Business, performance, information/data, application/service, and technology descriptions address security. Organization CIO has approved current version of EA. Committee or group representing the enterprise or the investment review board has approved current version of EA.	EA products are periodically updated. IT investments comply with EA. Organization head has approved current version of EA.
Attribute 4: Verifies satisfaction of commitment		EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.	Progress against EA plans is measured and reported.	Quality of EA products is measured and reported.	Return on EA investment is measured and reported. Compliance with EA is measured and reported.

Source: GAO.

Note: each stage includes all elements of previous stages.

FRAUD, WASTE, ABUSE AND MISMANAGEMENT
of Federal programs and resources hurts everyone.

Call the Office of Inspector General
HOTLINE
1 (866) 906-2446
or email OIG@uscp.gov
to report illegal or wasteful activities.

You may also write to:
Office of Inspector General
United States Capitol Police
499 S. Capitol St., S.W. Suite 345
Washington D.C. 20510

Please visit our website at
http://www.uscapitolpolice.gov/oig.php