



---

## **Exhibit 300: Capital Asset Plan and Business Case Summary**

### **Part I: Summary Information And Justification**

---

#### **Section A: Overview**

1. Date of submission: **Sep 8, 2008**
2. Agency: **452**
3. Bureau: **00**
4. Name of this Capital Asset: **Identity Management System (Security Management System)**
5. Unique Project (Investment) Identifier: **452-00-01-01-01-1005-00**
6. What kind of investment will this be in FY2010? **Mixed Life Cycle**
7. What was the first budget year this investment was submitted to OMB? **FY2006**
8. Provide a brief summary and justification for this investment, including a brief description of how this closes in part or in whole an identified agency performance gap: **The Smithsonian is upgrading and expanding the capabilities of its Identity Management System to support the mandates of Homeland Security Presidential Directive 12 (HSPD-12) and the supporting Federal Information Processing Standard (FIPS) 201. FIPS 201 provides standards for administrative procedures to be used to identify an individual's identity when issuing identification credentials. The Identity Management System assists the Office of Protection Services (OPS) with the issuance and management of Smithsonian identification cards to staff, contractors, and volunteers. OPS also uses Smithsonian Security Management Systems (SMS) (integrated with the Identity Management System) to monitor thousands of intrusion detection devices,; and to manage physical access throughout the Institutions facilities. The Office of Protection Services (OPS) provides protection and security services and operates programs for security management and criminal investigations at the Smithsonian Institution (SI) facilities in Washington, D.C., New York City, Panama, and various locations world-wide. Access to facilities is gained by inspection of ID cards by security staff. Further access within buildings is controlled by proximity card readers. Some photographic ID cards currently issued are proximity cards that can grant access to rooms/areas that are controlled by card readers. . Each proximity card reader is linked to of fourteen security management systems (one of two products) currently implemented throughout SI. SMSs are also connected to video management components that integrate intrusion detection and access control components with video cameras installed a various locations throughout the Institution. The Identity Management System specifically produces the ID Credential and was upgraded in FY08 to incorporate Enrollment (finger printing and identity collection) System. Specifically, OPS plans to continue to provide operations and maintenance systems**

**support to the Institution to: expand the Identity Management System (fingerprinting and identity collection) to all remote sites; interface the Identity Management System with the SI's Human Resources System; provide contractor services for Identity Management System security documentation, testing and SI Accreditation and Life Cycle Management Documentation; provide ongoing licensing and maintenance support.**

9. Did the Agency's Executive/Investment Committee approve this request? **yes**
  - a. If "yes," what was the date of this approval? **Jun 29, 2007**
10. Did the Project Manager review this Exhibit? **yes**
11. Contact information of Program/Project Manager?

Name **Hugh F. Meehan, Jr.**  
Phone Number **202 633-5685**  
E-mail **meehanh@si.edu**

- a. What is the current FAC-P/PM (for civilian agencies) or DAWIA (for defense agencies) certification level of the program/project manager? **Waiver Issued**
  - b. When was the Program/Project Manager Assigned? **Sep 30, 2007**
  - c. What date did the Program/Project Manager receive the FAC-P/PM certification? If the certification has not been issued, what is the anticipated date for certification? **Jan 1, 1901**
12. Has the agency developed and/or promoted cost effective, energy efficient and environmentally sustainable techniques or practices for this project. **yes**
  - a. Will this investment include electronic assets (including computers)? **yes**
  - b. Is this investment for new construction or major retrofit of a Federal building or facility? (answer applicable to non-IT assets only) **no**
    1. If "yes," is an ESPC or UESC being used to help fund this investment?
    2. If "yes," will this investment meet sustainable design principles?
13. If "yes," is it designed to be 30% more energy efficient than relevant code?
14. Does this investment directly support one of the PMA initiatives? **yes**

**Expanded E-Government**

  - a. Briefly and specifically describe for each selected how this asset directly supports the identified initiative(s)? **The Security Management System (SMS) ID Badging System initiative supports the Smithsonian strategic goal to modernize Smithsonian management systems and it supports HSPD-12. It will support the expanded e-government initiative by providing electronic validation of identity source documents, electronic scanning and storage of identity source documents, electronic storage of all paperwork, electronic scanning of fingerprint biometrics and transmittal to the OPM, and replacement of paper forms.**
15. Does this investment support a program assessed using the Program Assessment Rating Tool (PART)? (For more information about the PART, visit [www.whitehouse.gov/omb/part](http://www.whitehouse.gov/omb/part).) **no**
  - a. If "yes," does this investment address a weakness found during a PART review? If "yes," what is the name of the PARTed program?
  - b. If "yes," what rating did the PART receive?
16. Is this investment for information technology? **yes**

For information technology investments only:

16. What is the level of the IT Project? (per CIO Council PM Guidance) **Level 1**
17. In addition to the answer in 11(a), what project management qualifications does the Project Manager have? (per CIO Council PM Guidance) **(1) Project manager has been validated as qualified for this investment**
18. Is this investment or any project(s) within this investment identified as "high risk" on the Q4-FY 2008 agency high risk report (per OMB Memorandum M-05-23)? **no**
19. Is this a financial management system? **no**
- a. If "yes," does this investment address a FFMIA compliance area?
1. If "yes," which compliance area:
- b. If "no," what does it address?
20. If "yes," please identify the system name(s) and system acronym(s) as reported in the most recent financial systems inventory update required by Circular A-11 section 52
21. What is the percentage breakout for the total FY2010 funding request for the following?

Hardware **10**  
 Software **10**  
 Services **80**  
 Other **0**

22. If this project produces information dissemination products for the public, are these products published to the Internet in conformance with OMB Memorandum 05-04 and included in your agency inventory, schedules and priorities? **n/a**
23. Contact information of individual responsible for privacy related questions:

Name **Marsha Shaines**  
 Phone Number **202 633-5106**  
 Title **Acting General Counsel**  
 E-mail **shainesm@si.edu**

24. Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval? **yes**
25. Does this investment directly support one of the GAO High Risk Areas? **no**

**Section B: Summary of Spending**

1.

	<b>PY-1 and earlier</b>	<b>PY 2008</b>	<b>CY 2009</b>
Planning:	0.808	0	0
Acquisition:	0	0.836	0.01
Subtotal Planning & Acquisition:	0.808	0.836	0.01
Operations & Maintenance:	0	0	0.077
TOTAL:	0.808	0.836	0.087

Government FTE Costs	0	0	0
Number of FTE represented by Costs:	0	0	0

2. Will this project require the agency to hire additional FTE's? **yes**
  - a. If "yes", How many and in what year? **1 FTE - FY09**
3. If the summary of spending has changed from the FY2009 President's budget request, briefly explain those changes:

#### Section D: Performance Information

Performance Information Table							
Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
2007	Enhanced Management Excellence	Processes and Activities	Security Management	The number of identification cards issued to staff that meet Personal Identity Identification (PIV-I) control objectives.	0	Increase the number of ID cards issued that meet PIV-1 control objectives by 25% (Approx. new credentials issued each year)	TBD
2007	Enhanced Management Excellence	Customer Results	Accuracy of Service or Product Delivered	Initiate background check/fingerprinting processes for individuals that receive ID credential.	50%	Expand the number of background checks to new categories of staff by 25%	75%
2007	Enhanced Management Excellence	Mission and Business Results	Security Management	Improve the accuracy of the data capture in the identity proofing and registration process	85%	Increase the accuracy in the capturing of data by 15%	99%
2007	Enhanced Management Excellence	Technology	Reliability	Percentage of servers that are protected against viruses and are not routinely updated with operating system patches.	0	Increase the percentage of servers that have updated virus software and	100%

						approved operating system patches by 50%	
2008	Enhanced Management Excellence	Processes and Activities	Security Management	The percentage of credentials issued to staff that meet Personal Identity Identification (PIV-I) control objectives.	25%	Increase the percentage of credentials issued that meet PIV-1 control objectives to 75%	Contracted awarded 8/12/08 for this service; expected completion date 11/21/08
2008	Enhanced Management Excellence	Mission and Business Results	Security Management	Store all Identity Management information in compliance with HSPD12 (PIV I),	0	100%	Contracted awarded 8/12/08 for this service; expected completion date 11/21/08
2008	Enhanced Management Excellence	Customer Results	Accuracy of Service or Product Delivered	Initiate background check/fingerprinting processes for individuals that receive ID credential.	75%	Expand the number of background checks to new categories of staff by 25%	95%
2008	Enhanced Management Excellence	Technology	External Data Sharing	The percentage of electronically transmitted requests for National Agency Checks (NAC) to OPM	0	Increase the percentage of electronic NAC requests to OPM by 50%	Contracted awarded 8/12/08 for this service; expected completion date 11/21/08
2009	Enhanced Management Excellence	Mission and Business Results	Security Management	Ensure the integrity of the credential database records by pulling personnel data directly from the enrollment system and SMS	0	Increase the accuracy of the current enrollment system database and SMS database for 75% accuracy	Contracted awarded 8/12/08 for this service; expected completion date 11/21/08
2009	Enhanced Management Excellence	Customer Results	Accuracy of Service or Product Delivered	The percentage of fingerprints that need to be redone due to poor image	15%	Reduce the percentage needed for redoing	Contracted awarded 8/12/08

				quality (electronic versus manual fingerprinting)		fingerprints to 5%	for this service; expected completion date 11/21/08
2009	Enhanced Management Excellence	Processes and Activities	Efficiency	The number of sites with electronic fingerprint capturing capability	0	Expand the number of sites that will have electronic fingerprinting capability as required by design.	Contracted awarded 8/12/08 for this service; expected completion date 11/21/08
2009	Enhanced Management Excellence	Technology	External Data Sharing	The number of electronically transmit requests for National Agency Checks (NAC) to OPM	50%	Increase the number of electronic NAC request to OPM to 100%	Contracted awarded 8/12/08 for this service; expected completion date 11/21/08
2010	Enhanced Management Excellence	Mission and Business Results	Security Management	Design a complete and fully operational IDMS/CMS	0	100%	TBD
2010	Enhanced Management Excellence	Customer Results	Accuracy of Service or Product Delivered	The percentage of records stored in the IDMS/CMS	75%	Increase the percentage of records stored by 95%	TBD
2010	Enhanced Management Excellence	Processes and Activities	Efficiency	Reduce processing time for background check and credential issuance	20 minutes	Reduce processing time by 50%	TBD
2010	Enhanced Management Excellence	Technology	External Data Sharing	The number of records electronically transferred from the IDMS/CMS to the SMS	0	100% transfer of record data (specified fields) from the IDMS/CMS to the SMS	TBD

**Section F: Enterprise Architecture (EA)**

1. Is this investment included in your agency's target enterprise architecture? **yes**
  - a. If "no," please explain why?

2. Is this investment included in the agency's EA Transition Strategy? **yes**
  - a. If "yes," provide the investment name as identified in the Transition Strategy provided in the agency's most recent annual EA Assessment.  
**Identify Management System (Security Management System)**
  - b. If "no," please explain why?
3. Is this investment identified in a completed and approved segment architecture?  
**no**
  - a. If "yes," provide the six digit code corresponding to the agency segment architecture. The segment architecture codes are maintained by the agency Chief Architect. For detailed guidance regarding segment architecture codes, please refer to <http://www.egov.gov/>. **401-000**

**4. Service Component Reference Model (SRM) Table :**

Agency Component Name	Agency Component Description	FEA SRM Service Type	FEA SRM Component	Service Component Reused		Internal or External Reuse?	BY Funding Percentage
				Component Name	UPI		
C-CURE 800 COTS Product	Provides access data and information	Knowledge Management	Information Retrieval			Internal	0
C-CURE 800 and Max1000 COTS products	Facilitates collection of data and information	Knowledge Management	Knowledge Capture			Internal	30
C-CURE 800 and Max1000 COTS products	Supports the creation of film or electronic images	Visualization	Imagery			Internal	0
C-CURE 800 COTS products	Provides Standardized/Canned Reports	Reporting	Standardized / Canned			Internal	10
C-CURE 800 and Max1000 COTS products	Supports the interchange of information between multiple systems or applications	Data Management	Data Exchange			Internal	10
C-CURE 800 COTS products	Supports the population of a data source with external data	Data Management	Loading and Archiving			Internal	30
C-CURE 800 and Max1000 COTS products	Supports the security of an organization's employees	Human Resources	Health and Safety			Internal	10
C-CURE 800 COTS products	Supports the listing of employees and their whereabouts	Human Capital / Workforce Management	Workforce Directory / Locator			Internal	0
C-CURE	Supports obtaining	Security	Identification			Internal	10

800 COTS products	information about validating parties attempting to logon to a system or application for security purposes	Management	and Authentication				
C-CURE 800 and Max1000 COTS products	Supports management of permissions for accessing physical spaces	Security Management	Access Control			Internal	0
C-CURE 800 and Max1000 COTS products	Monitors access control panels	Communication	Event / News Management			Internal	0
C-CURE 800 and Max1000 COTS products	Supports the monitoring, administration, and usage of applications and enterprise systems from locations outside the immediate environment	Systems Management	Remote Systems Control			Internal	0

**5. Technical Reference Model (TRM) Table:**

<b>FEA SRM Component</b>	<b>FEA TRM Service Area</b>	<b>FEA TRM Service Category</b>	<b>FEA TRM Service Standard</b>	<b>Service Specification</b>
Information Retrieval	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System/C-Cure
Information Retrieval	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Information Retrieval	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Information Retrieval	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Information Retrieval	Component Framework	Interface	Static Display	C-CURE Application
Information Retrieval	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Knowledge Capture	Service Access and Delivery	Access Channels	Web Browser	MS Internet Explorer
Knowledge Capture	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System/C-CURE
Knowledge Capture	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Knowledge Capture	Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	Direct Connection / PTZ protocols
Knowledge Capture	Service Platform	Delivery Servers	Application	MS Windows



	and Infrastructure		Servers	
Knowledge Capture	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Knowledge Capture	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Knowledge Capture	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Max1000
Knowledge Capture	Component Framework	Interface	Static Display	C-CURE application
Imagery	Service Access and Delivery	Access Channels	Web Browser	MS Internet Explorer
Imagery	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Imagery	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Imagery	Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	Direct Connection / PTZ protocols
Imagery	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Imagery	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Imagery	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Imagery	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Max1000
Imagery	Component Framework	Interface	Static Display	C-CURE application
Standardized / Canned	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Standardized / Canned	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Standardized / Canned	Service Access and Delivery	Delivery Servers	Application Servers	MS Windows
Standardized / Canned	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Standardized / Canned	Component Framework	Interface	Static Display	C-CURE application
Standardized / Canned	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Data Exchange	Service Access and Delivery	Access Channels	Web Browser	MS Internet Explorer
Data Exchange	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Data Exchange	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Data Exchange	Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	Direct Connection / PTZ protocols

Data Exchange	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Data Exchange	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Data Exchange	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Data Exchange	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Max1000
Data Exchange	Component Framework	Interface	Static Display	C-CURE application
Loading and Archiving	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Loading and Archiving	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Loading and Archiving	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Loading and Archiving	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Loading and Archiving	Component Framework	Interface	Static Display	C-CURE application
Loading and Archiving	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Health and Safety	Service Access and Delivery	Access Channels	Web Browser	MS Internet Explorer
Health and Safety	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Health and Safety	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Health and Safety	Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	Direct Connection / PTZ protocols
Health and Safety	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Health and Safety	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Health and Safety	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Health and Safety	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Max1000
Health and Safety	Component Framework	Interface	Static Display	C-CURE application
Workforce Directory / Locator	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Workforce Directory / Locator	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Workforce Directory / Locator	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Workforce Directory	Service Platform	Database /	Database	Progress OpenEdge

/ Locator	and Infrastructure	Storage		
Workforce Directory / Locator	Component Framework	Interface	Static Display	C-CURE application
Workforce Directory / Locator	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Identification and Authentication	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Identification and Authentication	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Identification and Authentication	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Identification and Authentication	Service Platform and Infrastructure	Database / Storage	Database	Progress / OpenEdge
Identification and Authentication	Component Framework	Interface	Static Display	C-CURE application
Identification and Authentication	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Access Control	Service Access and Delivery	Access Channels	Web Browser	MS Internet Explorer
Access Control	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Access Control	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Access Control	Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	Direct Connection / PTZ protocols
Access Control	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Access Control	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Access Control	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Access Control	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Max1000
Access Control	Component Framework	Interface	Static Display	C-CURE application
Event / News Management	Service Access and Delivery	Access Channels	Web Browser	MS Internet Explorer
Event / News Management	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Event / News Management	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Event / News Management	Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	Direct Connection / PTZ protocols
Event / News Management	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Event / News Management	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Event / News	Service Platform	Hardware /	Embedded	Indal proximity

Management	and Infrastructure	Infrastructure	Technology Devices	cards and readers
Event / News Management	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Max1000
Event / News Management	Component Framework	Interface	Static Display	C-CURE application
Remote Systems Control	Service Access and Delivery	Access Channels	Web Browser	MS Internet Explorer
Remote Systems Control	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System / C-CURE client
Remote Systems Control	Service Access and Delivery	Delivery Channels	Intranet	TCP/IP
Remote Systems Control	Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	Direct Connection / PTZ protocols
Remote Systems Control	Service Platform and Infrastructure	Delivery Servers	Application Servers	MS Windows
Remote Systems Control	Service Platform and Infrastructure	Database / Storage	Database	Progress OpenEdge
Remote Systems Control	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Indal proximity cards and readers
Remote Systems Control	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Max1000
Remote Systems Control	Component Framework	Interface	Static Display	C-CURE application

6. Will the application leverage existing components and/or applications across the Government (i.e., USA.Gov, Pay.Gov, etc)? **no**
- a. If "yes," please describe.

---

## Part II: Planning, Acquisition And Performance Information

---

NACIS | Feb 9, 2009

**Section B: Risk Management (All Capital Assets)** Does the investment have a Risk Management Plan? **yes**

- a. If "yes," what is the date of the plan? **Mar 1, 2007**
- b. Has the Risk Management Plan been significantly changed since last year's submission to OMB? **no**
- c. If "yes," describe any significant changes:
2. If there currently is no plan, will a plan be developed? **yes**
  - a. If "yes," what is the planned completion date? **Jun 29, 2008**
3. If "no," what is the strategy for managing the risks?
4. Briefly describe how investment risks are reflected in the life cycle cost estimate and investment schedule: **All contractor risks are covered under the risk mitigation plan. Contractor activities are governed by Smithsonian security policies, the lifecycle methodology, the configuration management process**

and the enterprise architecture. Infrastructure standards, a clearly defined architecture and lifecycle methodology, and an understanding of best practices minimize much of the risk associated with the deployment of COTS packages and in house development. In addition, contractors are evaluated on assessment and mitigation of risk within their areas of control. The standard process for mitigating risks, when they occur, is the following. Prioritize the risk in context with other processes; Develop plans to mitigate the risk; Collect metrics on the plans ;Take steps to prevent a recurrence of the risk Life cycle cost estimate risks are mitigated through a phase-based project management approach where the scope of the project is re-evaluated for each phase with development of operating plan, and by conducting ongoing life cycle management reviews. Investment schedule risks are mitigated by allocating sufficient project management and technical resources to the project; developing detail task level project schedules; working closely with project sponsor to ensure functional resources are available to provide project guidance, information, and project support for the implementation; and working closely with the vendor to receive timely updates of software modules.