

## Exhibit 300: Capital Asset Summary

### Part I: Summary Information And Justification (All Capital Assets)

#### Section A: Overview & Summary Information

**Date Investment First Submitted:** 2012-02-29  
**Date of Last Change to Activities:** 2012-06-28  
**Investment Auto Submission Date:** 2012-02-29  
**Date of Last Investment Detail Update:** 2012-02-29  
**Date of Last Exhibit 300A Update:** 2012-07-31  
**Date of Last Revision:** 2012-08-31

**Agency:** 014 - Department of State      **Bureau:** 00 - Agency-Wide Activity

**Investment Part Code:** 02

**Investment Category:** 00 - Agency Investments

**1. Name of this Investment:** Security/Cyber Security Services

**2. Unique Investment Identifier (UII):** 014-000000048

#### Section B: Investment Detail

- 1. Provide a brief summary of the investment, including a brief description of the related benefit to the mission delivery and management support areas, and the primary beneficiary(ies) of the investment. Include an explanation of any dependencies between this investment and other investments.**

Cyber Security is a branch of technology known as information security as applied to computers and networks. The objective of cyber security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. Critical benefits resulting from the execution and utilization of cyber security technologies are reduced incidences of identity theft and PII compromise, reduced incidences of physical and infrastructure compromise, and protection against espionage or other malicious attacks. Cyber security is achieved through: 1. assessing the vulnerability of a network and associated applications; 2. identifying areas of weakness; 3. implementing plans and applications to control weaknesses; 4. performing operational analyses and incident monitoring; 5. conducting physical security assessments at remote sites of the network; 6. clearly define and communicate roles, responsibilities, and requirements of the network managers and users; 7. establish a configuration management process; and 8. manage risk. Activities performed and managed by the child initiatives support the Department of State's cyber security program. This major initiative encompasses the following initiatives: AIS Security Infrastructure Support Program, Anti-Virus Program (AV), Communications Security Audit Program (COMSEC), Electronic Key Management System (EKMS), In-Line Network Encryption (INE), Information Assurance Program (IA), Mainframe System Security Program (MSP), Public Key Infrastructure and

Biometrics Logical Access Development and Execution Program (PKI/BLADE), Red Switch, Role-Based Cyber Security Training, Secure Voice Program, and Technical Security and Safeguards (TSS).

**2. How does this investment close in part or in whole any identified performance gap in support of the mission delivery and management support areas? Include an assessment of the program impact if this investment isn't fully funded.**

The purpose of cyber security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, cyber security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Cyber Security increases the Department's ability to provide secure services to citizens, affect foreign affairs policy, and effectively manage information flows. If this initiative is not fully funded, the Department's ability to securely manage all of its resources will be critically compromised.

**3. Provide a list of this investment's accomplishments in the prior year (PY), including projects or useful components/project segments completed, new functionality added, or operational efficiency achieved.**

In addition to operating and maintaining the Department's Cyber Security Infrastructure, several projects in this initiative reached goals beyond the standard operational scope. Diplomatic Security's office of computer security won the SANS National Cyber Security Innovation Award. The Anti-virus program blocked 1 billion+ spam messages and eradicated 964 thousand viruses. They continue to detect approximately 6,222 risks a month. In 2011, 96% of State's COMSEC accounts were audited, 271 accounts received satisfactory ratings, 11 accounts received outstanding ratings and 19 accounts received unsatisfactory ratings. Deployment of the CARDS electronic distribution and accounting system to 100% of our end users was completed. This has resulted in a reduction in the distribution time of materials to our foreign missions from 30 days (via dip pouch) to real-time (electronically). The PKI BLADE office successfully deployed 99% of the ARRA funded PKI/BLADE card readers.

**4. Provide a list of planned accomplishments for current year (CY) and budget year (BY).**

This initiative plans to continue to provide operations and maintenance support for the Department's Cyber Security infrastructure. Specific accomplishments planned to be completed by the individual projects represent enhancements to the infrastructure, streamlining activities, and hardening activities to defend against malicious attacks. Security/Cyber Security services planned accomplishments include: Design and development of on-line classified equipment lifecycle management training module Support decommissioning and disposal of excess or obsolete classified TEMPEST IT equipment Implementation of Defensive Technical Counter-intelligence Safeguards and protective technologies Test various aspects of the DoS network for vulnerabilities to include conducting quarterly penetration testing and provision of ad hoc testing in response to requests. Renovate Cyber Incident Response Team facility to improve the working environment, prepare for future expansion, improve monitoring capability and take advantage of technology. Update Annual Cyber Security Awareness course (PS800) Obtain 90%

user compliance of Annual Cyber Security Awareness course (PS800) Symantec Endpoint Protection Manager Servers (SEPM) will be upgraded to Windows 2008 on OpenNet in 2012. Conduct Communication Security (COMSEC) audits on over 300 Department of State COMSEC accounts containing more than 130,000 items ensuring proper handling and accounting of National Security equipment and materials. Provide one-on-one refresh training to COMSEC account custodians and alternates domestically and overseas. Provide a centralized, web-based system which manages the distribution, accounting, and records management of COMSEC materials 24x7. Increase the efficiency of keying material distribution. Provide 100% accountability for 90,000 COMSEC items and maintain accurate records for 4,500 COMSEC cleared personnel. Support final reconfiguration of BIMC and HST for CSS primary and backup systems. Upgrade of z/OS to 1.11 in planning phase. Upgrade the Department's core DRSN switches with newer devices that allow for expanded capabilities. During this year, DTS also plans to connect the VoSIP network to outside agencies VoSIP networks. This connection will allow calls to be placed without the need of passing through the DRSN network.

5. **Provide the date of the Charter establishing the required Integrated Program Team (IPT) for this investment. An IPT must always include, but is not limited to: a qualified fully-dedicated IT program manager, a contract specialist, an information technology specialist, a security specialist and a business process owner before OMB will approve this program investment budget. IT Program Manager, Business Process Owner and Contract Specialist must be Government Employees.**

2012-01-20

## Section C: Summary of Funding (Budget Authority for Capital Assets)

1.

Table I.C.1 Summary of Funding

	PY-1 & Prior	PY 2011	CY 2012	BY 2013
Planning Costs:	\$0.4	\$0.4	\$0.4	\$0.4
DME (Excluding Planning) Costs:	\$86.9	\$0.1	\$0.1	\$0.1
DME (Including Planning) Govt. FTEs:	\$0.0	\$0.0	\$0.0	\$0.0
Sub-Total DME (Including Govt. FTE):	\$87.3	\$0.5	\$0.5	\$0.5
O & M Costs:	\$238.0	\$63.8	\$75.2	\$78.8
O & M Govt. FTEs:	\$12.6	\$9.2	\$12.8	\$9.4
Sub-Total O & M Costs (Including Govt. FTE):	\$250.6	\$73.0	\$88.0	\$88.2
Total Cost (Including Govt. FTE):	\$337.9	\$73.5	\$88.5	\$88.7
Total Govt. FTE costs:	\$12.6	\$9.2	\$12.8	\$9.4
# of FTE rep by costs:	439	198	198	200
Total change from prior year final President's Budget (\$)		\$70.3	\$85.2	
Total change from prior year final President's Budget (%)		2.00%	2.00%	

**2. If the funding levels have changed from the FY 2012 President's Budget request for PY or CY, briefly explain those changes:**

Funding levels have not changed from the FY President's Budget request.

Section D: Acquisition/Contract Strategy (All Capital Assets)

Table I.D.1 Contracts and Acquisition Strategy

Contract Type	EVM Required	Contracting Agency ID	Procurement Instrument Identifier (PIID)	Indefinite Delivery Vehicle (IDV) Reference ID	IDV Agency ID	Solicitation ID	Ultimate Contract Value (\$M)	Type	PBSA ?	Effective Date	Actual or Expected End Date
---------------	--------------	-----------------------	--	--	---------------	-----------------	-------------------------------	------	--------	----------------	-----------------------------

NONE

**2. If earned value is not required or will not be a contract requirement for any of the contracts or task orders above, explain why:**

Contract EVM requirements are explicitly discouraged for Fixed-Price contracts by DoD (the creator of EVM) as well as DHS, the next largest user of EVM. Published EVM guides and policies have been clear on that position for many years, and that is consistent with the regulations (FAR). That is because in a Fixed-Price environment, there is no cost variance to the government, so there is no cost/price variance to track, rendering a cost-based EVM exercise meaningless. In a Fixed-Price environment, the cost/price risk of cost overruns is entirely on the contractor, so the risk does not warrant the cost of requiring the contractor to report on EVMS. For the same reason, as well as to protect proprietary data, it is also inappropriate for the government to request detailed cost/price information (other than what was provided at time of award to support the initial price analysis) under a Fixed-Price contract.

## Exhibit 300B: Performance Measurement Report

### Section A: General Information

**Date of Last Change to Activities:** 2012-06-28

### Section B: Project Execution Data

**Table II.B.1 Projects**

Project ID	Project Name	Project Description	Project Start Date	Project Completion Date	Project Lifecycle Cost (\$M)
001	AIS Security Infrastructure Support Program	Provides technical cyber security operational support to the Department's IT infrastructure.			
002	Anti-Virus	Protects DoS global IT infrastructure from destructive programs by scanning each piece of email that transits the Gateway for malicious code.			
003	Communications Security Audit Program	Ensures audits are conducted for each ComSec account.			
004	Electronic Key Management System	Provides cryptographic keying material and equipment.			
005	In-Line Network Encryption	Procures, operates, and maintains Type 1 encryption devices required for the Department of State's classified communications.			
006	Information Assurance Program	Ensures the protection of IT assets (information and information systems) and the continuity of IT operations in support of DoS mission objectives.			

**Table II.B.1 Projects**

Project ID	Project Name	Project Description	Project Start Date	Project Completion Date	Project Lifecycle Cost (\$M)
007	Mainframe System Security Program	IT security program controlling communication between MSDC, BIMC, KCC and PFSC.			
008	Public Key Infrastructure and Biometrics Logical Access Development and Execution Program	Enables e-commerce, secures Web transactions and network devices, and provides privacy to users.			
009	Red Switch Program	Uses now-current technology to provide a single, integrated application that satisfies the current and future requirements of the annuitants and facilitates the work of the financial and personnel staff.			
010	Role-Based Cyber Security Training	This program provides role-based, instructor-led cyber security training to USG personnel and fulfills legal, Presidential and Department requirements.			
011	Secure Voice	Required for classified voice and data communications. NSA has identified the Sectera vIPer phone as the replacement unit for Secure Terminal Equipment (STE). The Sectera vIPer phone is a secure voice device designed to encrypt voice and data.			
012	Technical Security and Safeguards	TSS provides vital defensive technical security solutions critical to hardware security and infrastructure.			

**Activity Summary**

Roll-up of Information Provided in Lowest Level Child Activities

Project ID	Name	Total Cost of Project Activities (\$M)	End Point Schedule Variance (in days)	End Point Schedule Variance (%)	Cost Variance (\$M)	Cost Variance (%)	Total Planned Cost (\$M)	Count of Activities
------------	------	--	---------------------------------------	---------------------------------	---------------------	-------------------	--------------------------	---------------------

**Activity Summary**

Roll-up of Information Provided in Lowest Level Child Activities

Project ID	Name	Total Cost of Project Activities (\$M)	End Point Schedule Variance (in days)	End Point Schedule Variance (%)	Cost Variance (\$M )	Cost Variance (%)	Total Planned Cost (\$M)	Count of Activities
001	AIS Security Infrastructure Support Program							
002	Anti-Virus							
003	Communications Security Audit Program							
004	Electronic Key Management System							
005	In-Line Network Encryption							
006	Information Assurance Program							
007	Mainframe System Security Program							
008	Public Key Infrastructure and Biometrics Logical Access Development and Execution Program							
009	Red Switch Program							
010	Role-Based Cyber Security Training							
011	Secure Voice							
012	Technical Security and Safeguards							

**Key Deliverables**

Project Name	Activity Name	Description	Planned Completion Date	Projected Completion Date	Actual Completion Date	Duration (in days)	Schedule Variance (in days )	Schedule Variance (%)
007	Mainframe System Security Program	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%

Key Deliverables								
Project Name	Activity Name	Description	Planned Completion Date	Projected Completion Date	Actual Completion Date	Duration (in days)	Schedule Variance (in days )	Schedule Variance (%)
001	AIS Security Infrastructure Support Program	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
008	Public Key Infrastructure and Biometrics Logical Access Development and Execution Program	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
002	Anti-Virus	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
003	Communications Security Audit Program	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
009	Red Switch Program	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
004	Electronic Key Management System	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
010	Role-Based Cyber Security Training	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
005	In-Line Network Encryption	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
011	Secure Voice	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
006	Information Assurance Program	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
012	Technical Security and Safeguards	Operations and Maintenance	2012-03-30	2012-03-30		181	-154	-85.08%
012	Technical Security and Safeguards	Operations and Maintenance	2012-09-30	2012-09-30		182	0	0.00%
007	Mainframe System Security Program	Operations and Maintenance	2012-09-30	2012-09-30		182	0	0.00%
001	AIS Security Infrastructure Support Program	Operations and Maintenance	2012-09-30	2012-09-30		182	0	0.00%
008	Public Key	Operations and	2012-09-30	2012-09-30		182	0	0.00%

Key Deliverables								
Project Name	Activity Name	Description	Planned Completion Date	Projected Completion Date	Actual Completion Date	Duration (in days)	Schedule Variance (in days )	Schedule Variance (%)
	Infrastructure and Biometrics Logical Access Development and Execution Program	Maintenance						
003	Communications Security Audit Program	Operations and Maintenance	2012-09-30	2012-09-30		182	0	0.00%
009	Red Switch Program	Operations and Maintenance	2012-09-30	2012-09-30		182	0	0.00%
004	Electronic Key Management System	Operations and Maintenance	2012-09-30	2012-09-30		182	0	0.00%
010	Role-Based Cyber Security Training	Operations and Maintenance	2012-09-30	2012-09-30		182	0	0.00%
005	In-Line Network Encryption	Operations and Maintenance	2012-09-30	2012-09-30		182	0	0.00%
011	Secure Voice	Operations and Maintenance	2012-09-30	2012-09-30		182	0	0.00%

## Section C: Operational Data

Table II.C.1 Performance Metrics

Metric Description	Unit of Measure	FEA Performance Measurement Category Mapping	Measurement Condition	Baseline	Target for PY	Actual for PY	Target for CY	Reporting Frequency
Percentage of customer requests serviced in 30 minutes	Percentage	Customer Results - Timeliness and Responsiveness	Over target	98.000000	98.000000	99.000000	98.000000	Monthly
Authenticated and Authorization Breaches	Per Event	Mission and Business Results - Management of Government Resources	Under target	0.000000	0.000000	0.000000	0.000000	Monthly
Depot software upgrades.	Business Days	Technology - Reliability and Availability	Under target	5.000000	6.000000	6.500000	4.000000	Monthly
Depot Life Cycle Maintenance	Business Days	Process and Activities - Cycle Time and Timeliness	Under target	7.000000	7.000000	7.000000	7.000000	Quarterly
Customer Support Response Time	Business Days	Customer Results - Timeliness and Responsiveness	Under target	3.000000	3.000000	4.000000	2.000000	Quarterly
Global software deployments	Months	Process and Activities - Cycle Time and Timeliness	Under target	7.000000	9.000000	9.000000	3.000000	Semi-Annual
Keying Material Provisioning	Business Days	Mission and Business Results - Services for Citizens	Under target	30.000000	45.000000	40.000000	5.000000	Quarterly
Maintain Inventory of Operational Equipment	Percentage	Technology - Reliability and Availability	Over target	95.000000	95.000000	97.000000	97.000000	Semi-Annual
Efficiency of keying material distribution	Business Days	Customer Results - Timeliness and Responsiveness	Under target	3.000000	2.000000	2.000000	2.000000	Quarterly
Consistency in COMSEC Transactions	Number	Mission and Business Results - Services for Citizens	Over target	5.000000	4.000000	4.500000	3.000000	Monthly
Accountability all	Percentage	Mission and Business	Over target	100.000000	100.000000	100.000000	100.000000	Semi-Annual

Table II.C.1 Performance Metrics

Metric Description	Unit of Measure	FEA Performance Measurement Category Mapping	Measurement Condition	Baseline	Target for PY	Actual for PY	Target for CY	Reporting Frequency
COMSEC items		Results - Services for Citizens						