(U) CRYPTANALYSIS & EXPLOITATION SERVICES
(U) ANALYSIS OF TARGET SYSTEMS

This Exhibit is SECRET//NOFORN									
	FY 2011[1] Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding ($M)	39.4	35.1	—	35.1	34.3	—	34.3	-0.8	-2
Civilian FTE	240	211	—	211	201	—	201	-10	-5
Civilian Positions	240	211	—	211	201	—	201	-10	-5
Military Positions	2	2	—	2	2	—	2	—	—

[1]Includes enacted OCO funding. Totals may not add due to rounding.

(U) Project Description

(S//SI//REL TO USA, FVEY) The Analysis of Target Systems Project produces prototype capabilities to exploit new communications technologies and systems which are then integrated into the SIGINT system via the Exploitation Solutions Project in this Expenditure Center (EC). This Project enables the defeat of strong commercial data security systems; develops capabilities to exploit emerging information systems and technologies that are employed or may be employed by SIGINT targets; develops analytic algorithms, processes, and procedures to exploit emerging information systems technologies; and develops initial recognition, exploitation, and prototype solutions against new technology targets. This Project contains the Information Systems Analysis and Cryptanalytic Vulnerability Discovery & Exploitation Solutions Sub-Projects.

(U) Base resources in this project are used to:

- (S//SI//REL TO USA, FVEY) Conduct vulnerability analysis and develop exploitation capabilities against network communications protocols and commercial network security products, including protocol structure, authentication and access control, data integrity, and non-application layer encryption for integration into Endpoint and MidPoint access solutions for use against high-priority SIGINT targets.
- (TS//SI//REL TO USA, FVEY) Provide target exemplar secure communications products, both foreign and domestic produced, to pursue vulnerability analysis and develop exploitation capabilities against the authentication and encryption schemes.
- (S//SI//REL TO USA, FVEY) Support work to provide capabilities against emerging communications technologies through error correction, demodulation, reverse-engineering, multiplexers, and personal communications interfaces.
- (S//SI//REL TO USA, FVEY) Perform analysis of information security systems, products, and services in order to develop exploitation solutions designed to address customer-driven and anticipatory requirements.
- (S//SI//REL TO USA, FVEY) Anticipate future encryption technologies of SIGINT targets and prepare strategies to exploit those technologies.
- (TS//SI//REL TO USA, FVEY) Develop, enhance, and implement software attacks against encrypted signals.
- (TS//SI//REL TO USA, FVEY) Develop exploitation capabilities against specific key management and authentication schemes.
- (TS//SI//REL TO USA, FVEY) Analyze and develop exploitation capabilities against emerging multimedia applications (video, voice, fax, data compression, and file formats) and multiplexer capabilities.

- (TS//SI//REL TO USA, FVEY) Provide hardware and software tools for analyzing and developing methods of exploiting known or emerging information systems that are likely to be employed by targets to store, manage, protect, or communicate data of SIGINT values.
- (S//SI//REL TO USA, FVEY) Perform reverse-engineering of hardware and software-based encryption systems, develop reverse-engineering tools and techniques useful to the reverse engineering community at large, and provide cryptanalytic engineering services to the cryptanalytic community.
- (S//SI//REL TO USA, FVEY) Maintain state-of-the-art laboratory networks directly supporting analysis of application-layer encryption products, hardware reverse-engineering, communications systems analysis, simulation of target implementation scenarios, vulnerability detection, and cryptanalytic assistance to Computer Network Exploitation (CNE).
- (TS//SI//REL TO USA, FVEY) Develop cryptanalytic capabilities and provide comprehensive support to facilitate CNE operations against target systems and to facilitate offensive/defensive Computer Network Operations (CNO).
- (S//SI//REL TO USA FVEY) Create comprehensive CNO capabilities, including Radio Frequency (RF)-based, against highly mobile and re-configurable communications networks, and support their integration into multiple military service-level elements.
- (S//SI//REL TO USA, FVEY) Guide the future design and effective use of cryptanalytic computers to meet the needs of the cryptanalytic community.
- (S//SI//REL TO USA, FVEY) Support investment in reverse engineering through partnerships with National Laboratories and engineering services contractors.
- (S//SI//REL TO USA, FVEY) Develop initial recognition, exploitation, and prototype solutions against new technology targets. These capabilities are integrated into the processing and exploitation infrastructure or into customized tactical exploitation capabilities.
- (TS//SI//REL TO USA, FVEY) Develop methods to discover and exploit communication systems employing public key cryptography.
- (S//SI//REL TO USA, FVEY) Develop methods to exploit communications protected by passwords or pass phrases.
- (U//FOUO) Serve as the Cryptanalysis and Exploitation Services (CES) experts in the use of High Performance Computing hardware. Consult with other organizations on the most efficient utilization of these devices and participate in their design and development.
- (TS//SI//REL TO USA, FVEY) Develop exploitation processes for a variety of advanced communication security systems. These include Public Key Cryptography and Virtual Private Network (VPN) systems. Manage mature exploitation processes and develop tools to aid in exploitation of internet security protocols and administration.
- (U//FOUO) Provide for training in state-of-the-art computing technologies and travel for collaborative analysis and interaction with foreign and domestic partners.

(U) There are no new activities in this Project for FY 2013.

(U) The CCP expects this Project to accomplish the following in FY 2013:

- (S//SI//REL TO USA, FVEY) Develop new capabilities against 50 commercial information security device products to exploit emerging technologies.
- (TS//SI//REL TO USA, FVEY) Contribute to the design and development of four additional enabled solutions to help defeat data security systems that are used or may be used by SIGINT targets.

- (S//SI//REL TO USA, FVEY) Support SIGINT Forensics by extracting data from 10 additional hardware devices in support of prototype exploitation capability development.
- (S//SI//REL TO USA, FVEY) Develop 40 new capabilities (including new algorithms, processes and procedures) to exploit target information systems and technologies.
- (TS//SI// REL TO USA, FVEY) Develop 10 new capabilities to include new password recovery strategies, new password attacks on new hardware, automating password attacks, solving particular public-key crypt problems, discovering new targets that result in cryptanalytic gains for CES and developing new attacks against VPN technologies.