Published: September 5, 2013

Secret Documents Reveal N.S.A. Campaign Against Encryption

Documents show that the N.S.A. has been waging a war against encryption using a battery of methods that include working with industry to weaken encryption standards, making design changes to cryptographic software, and pushing international encryption standards it knows it can break. Related Article »

Excerpt from 2013 Intelligence Budget Request Bullrun Briefing Sheet

This excerpt from the N.S.A.'s 2013 budget request outlines the ways in which the agency circumvents the encryption protection of everyday Internet communications. The Sigint Enabling Project involves industry relationships, clandestine changes to commercial software to weaken encryption, and lobbying for encryption standards it can crack.

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

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)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—

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

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and technical challenges of discovering and successfully exploiting systems of interest within the ever-more integrated and security-focused global communications environment.

(TS//SI//REL TO USA, FVEY) This Project supports the Comprehensive National Cybersecurity Initiative (CNCI) by investing in corporate partnerships and providing new access to intelligence sources, reducing collection and exploitation costs of existing sources', and enabling expanded network operation and intelligence exploitation to support network defense and cyber situational awareness. This Project contains the SIGINT Enabling Sub-Project.

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

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.
- (U//FOUO) Maintain understanding of commercial business and technology trends.
- (U//FOUO) Procure products for internal evaluation.
- (U//FOUO) Partner with industry and/or government agencies in developing technologies of strategic interest to NSA/CSS.

The N.S.A.'s Sigint Enabling Project is a $250 million-a-year program that works with Internet companies to weaken privacy by inserting back doors into encryption products. This excerpt from a 2013 budget proposal outlines some methods the agency uses to undermine encryption used by the public.

The agency works with companies to insert back doors into the commercial products. These back doors allow the agency, and in theory only the agency, to gain access to scrambled information that it would not be able to view otherwise.

Because the N.S.A. has long been considered the world's top authority on encryption, it has dual, sometimes competing, roles. One responsibility of the agency is to safeguard United States communications by promoting encryption standards, and the other is to break codes protecting foreign communications. Part of the Sigint Enabling Project's goal is to influence these standards — which are often used by American companies — and weaken them.

- (TS//SI//REL TO USA, FVEY) Support the SIGINT exploitation of NGW, a MIP/NIP collective investment. This request reflects only the NIP portion of the program. Refer to MIP NSA volume for details on MIP related activities.
- (TS//SI//REL TO USA, FVEY) Provide for continued partnerships with major telecommunications carriers to shape the global network to benefit other collection accesses and allow the continuation of partnering with commercial Managed Security Service Providers and threat researchers, doing threat/vulnerability analysis.
- (TS//SI//REL TO USA, FVEY) Continue relationships with commercial IT partners and capitalize on new opportunities, including the enabling of cryptography used by the [redacted] governments; enable the encryption being used in a high interest satellite signal, which allows access to the communications being carried on a commercial satellite provider.

(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:

- (TS//SI//NF) Reach an initial operating capability for SIGINT access to data flowing through a commercial Arabic language/Middle East-oriented anonymous internet service. [CCP_00009]
- (TS//SI//REL TO USA, FVEY) Reach full operating capability for SIGINT access to data flowing through a hub for a major commercial communications provider and assess its long term benefits.
- (TS//SI//REL TO USA, FVEY) Reach full operating capability for SIGINT access to a major Internet Peer-to-Peer voice and text communications system.
- (TS//SI//REL TO USA, FVEY) Complete enabling for [redacted] encryption chips used in Virtual Private Network and Web encryption devices. [CCP_00009]
- (TS//SI//REL TO USA, FVEY) Make gains in enabling decryption and Computer Network Exploitation (CNE) access to fourth generation/Long Term Evolution (4G/LTE) networks via enabling. [CCP_00009]
- (TS//SI//REL TO USA, FVEY) Assess existing wireless calling metadata accesses and balance flow of this data into NSA/CSS with the ability to ingest and utilize this information. [CO_00047]
- (TS//SI//REL TO USA, FVEY) Assess existing commercial cyber information flows and balance the flow of this data into NSA/CSS with the ability to ingest and analyze this information to support cyber situational awareness. [CO_00047]
- (TS//SI//NF) Shape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS. [CCP_00090]

(U) Changes From FY 2012 to FY 2013:

(S//NF) SIGINT Enabling: -$20.4 million (-$20.4 Base), -2 civilian positions. The aggregate decrease is the result of:

- (U) Increases:
  - (TS/SI//NF) $5.6 million reflects additional level of investment in enabling exploitation capabilities against NGW mobile and data networks.
  - (TS//SI//NF) $4.1 million enables additional support to Endpoint operations. Support to this mission area requires SIGINT Enabling to invest in new infrastructure and capabilities with commercial partners.
  - (S//NF) $0.4 million in civilian pay and benefits.

The agency defines capability as “the NSA/CSS ability to exploit a specific technology,” according to a 2010 document outlining the Bullrun program. Here, the agency is claiming that it can gain access to the text and audio of an Internet chat service. It is unclear from the documents that The New York Times and ProPublica have access to which service this document refers to.

Large Internet companies use dedicated hardware to scramble traffic before it is sent. In 2013, the agency planned to be able to decode traffic that was encoded by one of these two encryption chips, either by working with the manufacturers of the chips to insert back doors or by exploiting a security flaw in the chips' design.

— (S//NF) $0.3 million due to revised economic assumptions.

- (U) Decreases:
  - — (TS//SI//NF) $20.8 million of contractor reductions to fund priority Community investments, which impacts the ability to sustain and expand activities directly supporting cyber informational needs.
  - — (TS//SI//NF) Decrease of $10.0 million in support of deficit reduction efforts, which reduces effectiveness of accesses supporting intelligence collection and Endpoint operations.
  - — (TS//SI//NF) Two civilian positions reduces development of strategic capabilities enabling cryptographic exploitation of target communications to advance NSA/CSS' missions.

SIGINT Enabling Project Budget Chart **FY 2013 Budget Request by Appropriation Account** **This Exhibit is SECRET//NOFORN**			**Funds — Dollars in Millions**		
Subproject	**Description**	**Resourcing**	**FY 2011**	**FY 2012**	**FY 2013**
Operation and Maintenance, Defense-Wide		***Funds***	***139.53***	***104.86***	***118.52***
		Positions	***137***	***132***	***141***
SIGINT Enabling	Communications and Utilities	Base	0.02	—	—
	Contract Services	Base	116.41	75.53	85.88
	Equipment	Base	2.89	10.30	11.19
	Pay and Benefits	Base	18.67	17.94	19.81
	Supplies and Materials	Base	0.06	0.15	0.15
	Travel and Transportation	Base	1.47	0.95	1.50
		Positions	137	132	141
Research, Development, Test, and Evaluation, Defense-Wide		***Funds***	***159.08***	***170.51***	***136.42***
		Positions	***7***	***11***	***—***
SIGINT Enabling	Communications and Utilities	Base	0.11	—	—
	Contract Services	Base	155.89	166.25	129.10
	Equipment	Base	1.82	2.66	7.21
	Pay and Benefits	Base	1.05	1.50	—
	Supplies and Materials	Base	<0.01	0.10	0.10
	Travel and Transportation	Base	0.20	—	—
		Positions	7	11	—
Totals may not add due to rounding.					