

~~TOP SECRET//SI//TK//RSEN//NOFORN~~

National Intelligence Program

FY 2015
Congressional Budget Justification



Volume XIII

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

MARCH 2014



DRV FROM: Multiple Sources
DECL ON: 20390306

~~TOP SECRET//SI//TK//RSEN//NOFORN~~

~~(S)~~ SPECIAL TOPIC
~~(U)~~ IC IT ENTERPRISE (IC ITE)

~~(U)~~ Roles and Responsibilities

~~(S)~~ Introduction and Background

~~(U//FOUO)~~ IC Information Technology Enterprise (IC ITE) represents the IC's investment in changing the culture to promote intelligence integration and information at the community level. NGA sees the success of the IC ITE initiative as an opportunity to increase investment and focus on the agency's core competency, GEOINT. As an IC ITE service provider and adopter, NGA is a strategic player in ensuring the success of this initiative. Partnered with DIA, NGA provides EMT and DTE services to the community. As much as possible, NGA has subscribed to the other services. While the tactical advantages are slight at this early stage, the strategic investment in the community is critical to the success of the IC ITE initiative.

~~(U)~~ IC Desktop Environment (IC DTE)

~~(U//FOUO)~~ IC DTE features a common desktop look and feel for all users, thick and thin client. Users will experience a single sign-on and can operate using the same email and secure phone for the duration of their career. A common set of office automation, communication, and collaboration tools will be available to increase information sharing and interoperability between agencies, as well as access to legacy applications, data, and services. The numerous features delivered by IC DTE are:

- ~~(S)~~ Unified Communications (interface between voicemail and email)
- ~~(S)~~ One secure phone number assigned for one's IC career
- ~~(S)~~ Mobile desktop (i.e., log in at any IC site where DTE has been implemented) and print capability (i.e., print locally)
- ~~(U)~~ Community-wide Global Address List
- ~~(S)~~ Standard Classification Management Tool
- ~~(S)~~ Home directories and profiles
- ~~(S)~~ Virtual Desktop Infrastructure
- ~~(S)~~ Mobile devices
- ~~(S)~~ Electronic content and records management
- ~~(U)~~ Improved security posture
- ~~(U)~~ Enhanced collaboration with community members and data stores

(b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142

(U) The expected benefits of IC DTE as part of the IC ITE are:

- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142

(U) Enterprise Management (EMT)

(U) Supports the current integrated service provider Change Control Board to process change requests coming from IC ITE Initial Operating Baseline in accordance with the IC ITE Change Control Process.

(U) The joint DIA/NGA EMT effort will provide cost efficiencies for the IC while delivering improved user experience. The vision is to facilitate a "one number to call" centralized IT operations with real-time health and status situational awareness across the entire IC ITE shared space. EMT also supports the current integrated service provider Change Control Board to process change requests coming from IC ITE Initial Operating Baseline in accordance with the IC ITE Change Control Process.

(U) As the transition progresses, the IC will benefit from EMT services in multiple ways:

- ~~(U//FOUO)~~ Better coordination between IC ITE service providers by establishing common processes to enable interoperability and consolidate service desk reporting.
- ~~(U//FOUO)~~ Reduced costs through use of a single, coherent view of the service providers' status, providing transparency and clear accountability for the level of service.
- ~~(U//FOUO)~~ Reduced risk by providing a focal point for enterprise risk analysis, and coordinated problem management analysis, to determine root causes for system outages. A formal coordinated change management process will reduce downtime and risk of operational failure.

~~(U)~~ Other NGA IC ITE Roles

~~(U//FOUO)~~ NGA is a consumer for the other IC ITE services provided by the other IC members. NGA's FY 2015 overall budget request includes resources for preparing data and applications for migrating to cloud and applications mail services. These resources will support the operation and sustainment of existing NGA enterprise capabilities, but will also be leveraged to transition to the IC ITE framework. These efforts include:

- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142

~~(U)~~ FY 2015 Budget Request

~~(U)~~ This section includes IC ITE service provider information directly related to the FY 2015 budget request.

(b)(1)

(b)(1)

(b)(1)

~~(U)~~ Expected Accomplishments

(b)(3):50 U.S.C. § 3142

(b)(3):50 U.S.C. § 3142

(b)(3):50 U.S.C. § 3142

~~(U)~~ IC Enterprise Management

- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

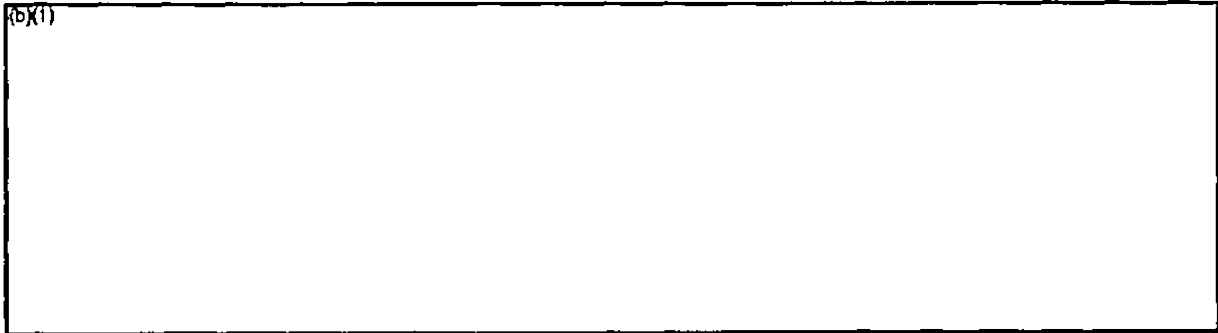
- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

~~(S)~~ SPECIAL TOPIC
~~(S)~~ CYBER ACTIVITIES MAPPED TO OMB TAXONOMY
~~(L)~~ Cyber Overview

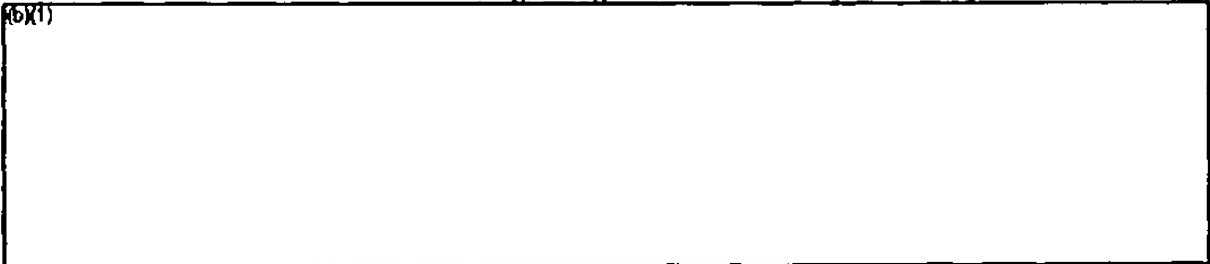
~~(S)~~ Mission

(b)(1)



~~(S)~~ The NGP Cybersecurity program ensures that all National System for Geospatial-Intelligence (NSG) networks, IT systems, and geospatial data worldwide are safe, secure, and compliant with applicable laws and regulations. In addition, cybersecurity efforts defend NSG networks and perimeter from cyber intrusions from state and non-state actors and guard against national security breaches by adversaries.

(b)(1)



~~(L)~~ OMB Cyber Taxonomy

~~(U//FOUO)~~ Effective FY 2014, OMB adopted a cyber-taxonomy for cyber activities that includes all activities formerly identified within the Comprehensive National Cybersecurity Initiative (CNCI), some specific FISMA resource data, and all other cyber activities or operations. The NGP has no activities that were not previously counted as CNCI nor does it have any activities that have been removed from the cyber program resulting from the new taxonomy.

~~(L)~~ FY 2015 Request

(b)(1)



- (b)(1)
-
-
-
-
-
-
-
-
-

Funding also provides:

- ~~(U//FOUO)~~ GEOINT crisis support and in-depth research on cyber threats.
- (b)(1)
-
- ~~(U//FOUO)~~ Support transition from DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, to IC Directive 503, Intelligence community Information Technology Systems Security Risk Management, Certification and Accreditation per public law.

~~(U)~~ Cybersecurity

~~(U)~~ Description

(b)(1)

~~(U//FOUO)~~ The NGP Cyber Security program ensures that all NSG networks, IT systems, and geospatial data worldwide are safe, secure and compliant with applicable laws and regulations. In addition, cyber security efforts defend NSG networks and perimeter from cyber intrusions from state and non-state actors and guard against national security breaches by adversaries.

(b)(1)

~~(U//FOUO)~~ NGA is also aggressive in protecting NSG information and systems from compromise. This includes monitoring systems for potential misuse, violations of policy, data exfiltration, malicious code and data spills.

~~(U)~~ Specifically, FY2015 resources will:

- (b)(1)
-
-
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

- (b)(1)
-
-
-
-
-
-

- (b)(3):50 U.S.C. § 3142

- (b)(3):50 U.S.C. § 3142

- (b)(1)
-
-
-
-

(b)(1)

~~(U)~~ **Accomplishments**

~~(U)~~ In FY 2013, NGP accomplishments in cyber security included the following:

- (b)(1)
-
-
-
-
-
-
-
-

- ~~(U//FOUO)~~ (b)(3):50 U.S.C. § 3142
- ~~(U//FOUO)~~ Continued to improve NGA cyber defenses using NGA enterprise-controlled interface and enterprise cross-domain platforms at the NCE.
- ~~(U//FOUO)~~ Continued NGA, ODNI, and DoD support for A&A efforts.

- (b)(1)
-
-
-
-
-

(b)(1)

-
-
-
-
-
-
-
-
-
-

(U) In FY 2014, NGP expects to accomplish the following:

- (b)(1)
-
-

- (U//FOUO) (b)(3):50 U.S.C. § 3142
- (U//FOUO) (b)(3):50 U.S.C. § 3142
- (b)(3):50 U.S.C. § 3142
- (U//FOUO) Continue NGA, ODNI, and DoD support for Assessment and Authorization (A&A) efforts.
- (S//NF) Maintain a 90 percent accreditation rating for FISMA reportable systems.

- (b)(1)
-
-

- ~~(U//FOUO)~~ Establish an NGA Office of Security Forensic Lab at NGA's West location and reach initial operating capability (IOC). This will serve as the primary forensic lab for the Office of Security in St. Louis and the COOP location for the Forensic Lab at NCF. It will process and investigate requests related to Personal Electronic Device (PED) entry into SCIF space, as well as requests from CSOC related to malicious activity on NGA networks.

(U) The NGP expects to accomplish the following outcomes in FY 2015:

- ~~(U//FOUO)~~ Continue to develop a formalized GEOINT cyber analysis training program to ensure GEOINT cyber analysts have a working-level understanding of technical aspects of cyber operations and network defense as well as an understanding of GEOINT tradecraft as it relates to cyber analysis.

- (b)(1)
-

- ~~(U//FOUO)~~ Achieve cyber-defense goal of 100 percent with no successful intrusions to prevent cyber intrusions into NGA networks from state and non-state actors and to guard against national security breaches of NGA networks by adversaries.
- ~~(U//FOUO)~~ Enhance NGA cyber defenses by adding additional functionality to the Enterprise Controlled Interface and fully instantiating the Enterprise Cross Domain Service at the NGA Campus East (NCE) and NGA Campus West (NCW). The Enterprise Controlled Interface provides centrally monitored, managed, and scalable perimeter defense capabilities at all security domains. The Enterprise Cross Domain Service implements low-to-high and high-to-low, redundant, load-balanced data and audited transfer services, to include support for National System for Geospatial-Intelligence Consolidated Library, and consolidates 70 percent to 80 percent of targeted systems.
- ~~(U//FOUO)~~ Strengthen the Intrusion Detection System (IDS) on NGA networks to mitigate insider threats and fortify NGA cyber defenses (e.g., prevent malicious attacks, thwart malware intrusions, track cyber-attack messages to origin, upgrade tools for detection of data tampering) to enable information sharing in a trusted secure environment.
- ~~(U//FOUO)~~ Develop and transition to an NSG enterprise-wide security access and control system. This will meet IC and DoD objectives for information sharing (ICD 501).
- ~~(U//FOUO)~~ Maintain IdAM as the enterprise authentication service; continue to expand interfaces with NSG systems, capabilities, and services, to include multiple security domains.
- ~~(U//FOUO)~~ Support the transition from (b)(3):50 U.S.C. § 3142
(b)(3):50 U.S.C. § 3142
(b)(3):50 U.S.C. § 3142 Certification and Accreditation per public law.

(b)(1)

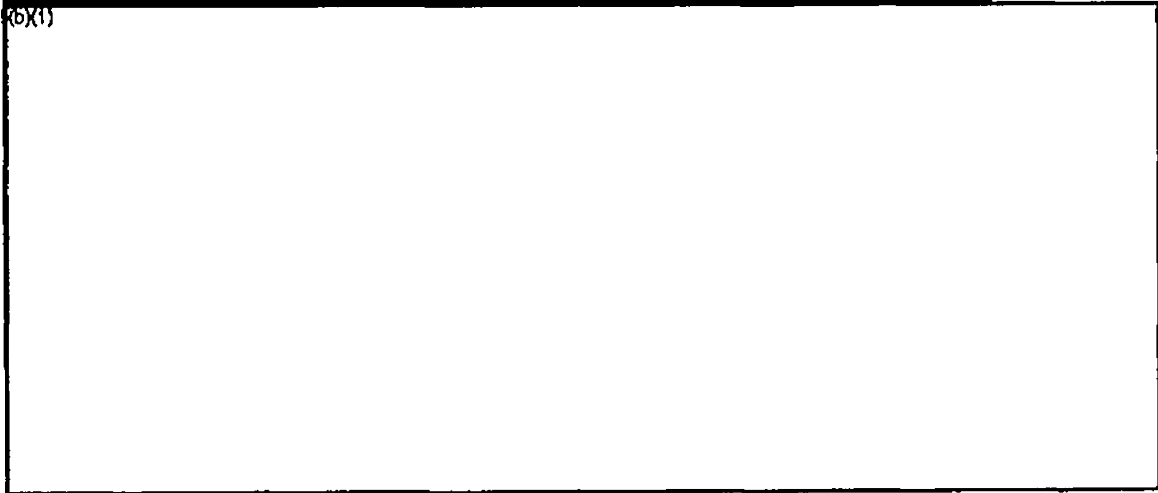
-
-
-
-
-

- ~~(U//FOUO)~~ Reach FOC in NGA Office of Security Forensic Lab-West.
- ~~(U//FOUO)~~ Establish an enterprise forensic capability in the NGA Office of Security Forensic Lab-West.
- ~~(U//FOUO)~~ Enhance the NGA Security's malware reverse engineering capability and reach initial operating capability (IOC).

(b)(1)

-
-

~~(U)~~ Cybersecurity Resource Summary



~~(S)~~ Cyber Operations

~~(S)~~ Description

~~(U//FOUO)~~ NGP cyber operations include the research and development of the necessary requirements to exploit current, new, and future sensors systems in ways that support new analytic tradecraft (GEOINT Sources, Sensors and Phenomenologies) to operationalize the visualization of cyber related infrastructure and network topology in three dimensions. Specifically, FY15 resources will be used to:

- ~~(U//FOUO)~~ Develop a capability to operationalize GEOINT data extracted from cyber-sourced raw data and build cyber topologies with automated mapping translation capabilities to support GEOINT analysis on hard intelligence problems.

~~(U)~~ Accomplishments

~~(U)~~ In FY 2013 and FY 2014, NGP accomplishments in cyber operations included the following:

- ~~(U//FOUO)~~ There was no NGP funding in cyber operations for FY 2013 or FY 2014.

~~(U)~~ The NGP expects to accomplish the following outcome in FY 2015:

- ~~(U//FOUO)~~ Operationalize GEOINT data extracted from cyber-sourced raw data and build cyber topologies with automated mapping translation capabilities to support GEOINT analysis on hard intelligence problems.

~~(S)~~ Cyber Operations Resource Summary

(b)(1)



(b)(1)

