



February 18, 2020

MR. JOHN GREENEWALD, JR.
THE BLACK VAULT
SUITE 1203
27305 WEST LIVE OAK ROAD
CASTAIC, CA 91384

FOIPA Request No.: 1448188-000
Subject: ITB Year in Review
(Fiscal Year 2013)

Dear Mr. Greenewald:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemption boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

Section 552		Section 552a
<input type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)	<input type="checkbox"/> (d)(5)
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)	<input type="checkbox"/> (j)(2)
<input type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)	<input type="checkbox"/> (k)(1)
_____	<input type="checkbox"/> (b)(7)(D)	<input type="checkbox"/> (k)(2)
_____	<input checked="" type="checkbox"/> (b)(7)(E)	<input type="checkbox"/> (k)(3)
_____	<input type="checkbox"/> (b)(7)(F)	<input type="checkbox"/> (k)(4)
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)	<input type="checkbox"/> (k)(5)
<input type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)	<input type="checkbox"/> (k)(6)
<input checked="" type="checkbox"/> (b)(6)		<input type="checkbox"/> (k)(7)

44 pages were reviewed and 43 pages are being released.

Please see the paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

- Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].
- This information has been referred to the OGA(s) for review and direct response to you.
- We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. "Part 1" of the Addendum includes standard responses that apply to all requests. "Part 2" includes additional standard responses that apply to all requests for records about yourself or any third party individuals.

“Part 3” includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Sixth Floor, 441 G Street, NW, Washington, D.C. 20001, or you may submit an appeal through OIP’s FOIA online portal by creating an account on the following website: <https://www.foiaonline.gov/foiaonline/action/public/home>. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked “Freedom of Information Act Appeal.” Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769. Alternatively, you may contact the FBI’s FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state “Dispute Resolution Services.” Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

See additional information which follows.

The enclosed documents represent the final release of information responsive to your Freedom of Information/Privacy Acts (FOIPA) request.

This material is being provided to you at no charge.

Sincerely,



David M. Hardy
Section Chief
Record/Information
Dissemination Section
Information Management Division

Enclosures

FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.

Part 1: The standard responses below apply to all requests:

- (i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on the www.fbi.gov/foia website.
- (ii) **Intelligence Records.** To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that any such records do or do not exist.

Part 2: The standard responses below apply to all requests for records on individuals:

- (i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.
- (ii) **Requests for Records about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.
- (iii) **Requests for Records for Incarcerated Individuals.** The FBI can neither confirm nor deny the existence of records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA exemptions (b)(7)(E), (b)(7)(F), and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (b)(7)(F), and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

- (i) **Record Searches.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems or locations where responsive records would reasonably be found. A standard search normally consists of a search for main files in the Central Records System (CRS), an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. Unless specifically requested, a standard search does not include references, administrative records of previous FOIPA requests, or civil litigation files. For additional information about our record searches, visit www.fbi.gov/services/information-management/foipa/requesting-fbi-records.
- (ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.
- (iii) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheet. These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.
- (iv) **National Name Check Program (NNCP).** The mission of NNCP is to analyze and report information in response to name check requests received from federal agencies, for the purpose of protecting the United States from foreign and domestic threats to national security. Please be advised that this is a service provided to other federal agencies. Private Citizens cannot request a name check.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1448188-0

Total Deleted Page(s) = 1
Page 37 ~ b6; b7C;

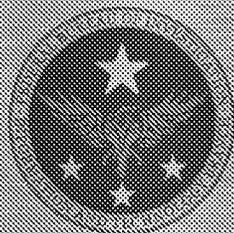
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

U.S. Department of Justice
Federal Bureau of Investigation
Information and Technology Branch



ITB

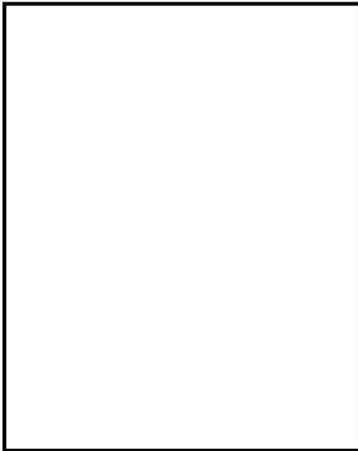
YEAR IN REVIEW



FISCAL YEAR

2013





Letter from the Executive Assistant Director and Chief Information Officer

b6
b7C

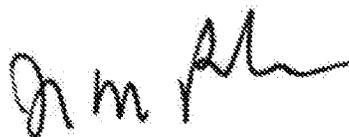
This report highlights many of the projects, programs, and initiatives that took place during Fiscal Year (FY) 2013. Despite being faced with extraordinary challenges including tight budget scenarios; hiring freezes; furloughs; and travel and training restrictions, dedicated and resourceful ITB employees stepped forward to find cost-effective innovative solutions to minimize the impact to the mission-critical services essential to our customers.

The ITB's global presence includes supporting IT requirements enterprise-wide – to 56 Field Offices, 381 Resident Agencies, and 78 Legal Attachés; managing more than 114,000 workstations; and providing an array of IT products and services to more than 36,000 employees and task force members. This is not an easy task. The ITB continued close coordination efforts with the field to listen to and ascertain what they need to support current and future law enforcement and intelligence community priorities.

The accomplishments in this report demonstrate the ITB's commitment to deliver leading-edge capabilities in case management, data management, and mobility. The focus of current modernization efforts is to move the FBI toward an agile, responsive, and efficient services-based operating model, emphasizing reuse of enterprise services both to increase cost savings and to enhance the reliability of IT infrastructure and applications.

Working together, I remain confident in the year ahead we will have opportunities to implement positive changes in the way the FBI conducts business.

I thank you for your continued partnership and trust.



Jerome M. Pender
Executive Assistant Director and
Chief Information Officer

6 ORGANIZATIONAL OVERVIEW

- 6 ITB's Senior Leadership
- 7 ITB Executive Staff Changes
- 7 Deputy Assistant Director John Hope Retires
- 8 ITB Organizational Chart FY 2013

10 STRATEGIC GUIDANCE

- 10 Strategy Management System
- 10 CIO Initiatives
- 11 Quarterly IT Business Reviews
- 11 Enterprise Data Management Office
- 12 Life Cycle Management
- 13 IT Asset Management Program
- 14 FBI's Enterprise IT Governance Framework
- 14 Bureau IT Knowledge Repository

14 PROJECTS, PROGRAMS, AND INITIATIVES

- 14 b7E
- 15 Electronic Laboratory Program
- 16
- 16 Human Resource Source
- 16 b7E
- 17 National Gang Intelligence Center-Information System
- 17 Next Generation Name Check Program
- 18 Sentinel
- 18 SharePoint 2010 Migration
- 19 Smartphone - Mobility
- 19 Microsoft® Windows®7 Operating System
- 20 Unified Financial Management System

20 INFRASTRUCTURE MODERNIZATION

- 20 Centralized Tiered Storage
- 20 Enterprise Circuit Consolidation Network Consolidation Efforts
- 21 Enclave Consolidation Initiative
- 21 Enterprise Remote Access Service
- 21 Printer Refresh
- 22 Next Generation Sensitive Compartmented Information Operational Network Deployment
- 22 b7E

22 SECURITY MANAGEMENT

- 22 Classification Management Tool
- 23 e-Discovery
- 23 Facility Security System
- 23 Provisioning and Access Control
- 24 Public Key Infrastructure Virtualization

25 AWARDS AND RECOGNITIONS

- 25 Attorney General's Award
- 25 Director's 2013 Annual Awards
- 26 IT Services Division Captures Top IT Innovator Award for Distributed Application Virtual Environment and Centralized Tiered Storage
- 27 2013 Computerworld Honors Program
- 27 Knowledge Awards Program
- 28 Employee Awards and Recognitions
- 28 2012 Office of the Director of National Intelligence Science and Technology Award Winners

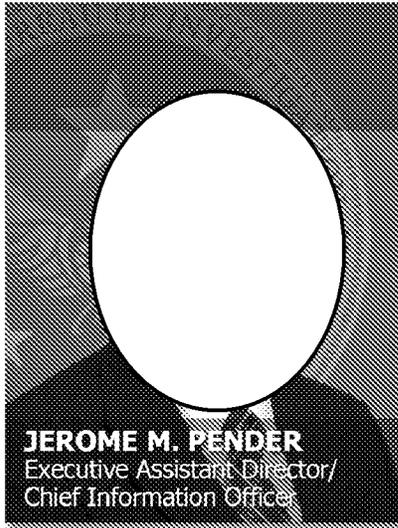
28 COLLABORATIVE FORUMS AND EVENTS

- 28 ITB All-Hands Meetings
- 30 IT Management Division's Shadow Week
- 30 Virtual IT Exchange Seminar
- 30 Cyber Table-top Exercise
- 31 Advanced Technology Group: Leveraging Technical Expertise
- 32 Damascus Students Participate in IT Job Shadow Day
- 33 Vendor Days
- 34 Combined Federal Campaign
- 35 ITMD Shines in the National Police Week 5K Race
- 36 Family Day

30 ACRONYMS AND CHARTS

- 38 Acronyms
- 40 History of Office of the Chief Information Officer/Information and Technology Branch FY2001-FY2006
- 42 History of Office of the Chief Information Officer/Information and Technology Branch FY2007-FY2012

EAD/CIO



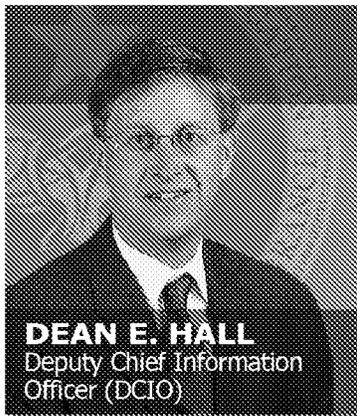
JEROME M. PENDER
Executive Assistant Director/
Chief Information Officer

MISSION:

- Deliver reliable and effective technology solutions needed to fulfill the FBI's mission anytime, anywhere, on-time, and on-budget;
- Lead the strategic directions for the FBI's Information Technology (IT) through the IT Strategic Plan, IT Portfolio management, IT Governance process; and
- Promote and facilitate the creation, sharing, and application of FBI knowledge products to improve overall effectiveness.

b6
b7c

DCIO



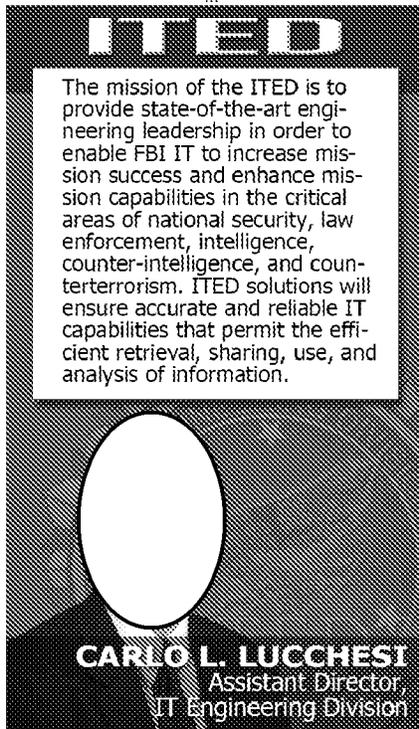
DEAN E. HALL
Deputy Chief Information Officer (DCIO)

The mission of the DCIO is consistent with that of the CIO. It is to provide leadership, policy guidance, and strategic direction for the FBI's IT enterprise.

The Information and Technology Branch (ITB) consists of three distinct divisions; the IT Engineering Division (ITED), IT Management Division (ITMD), and IT Services Division (ITSD). These components collaborate with each other to provide cradle-to-grave leadership and management of essential/critical IT programs, projects, and initiatives.

ITED

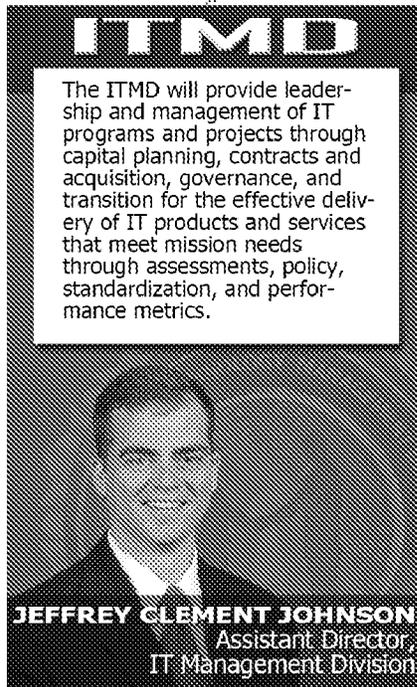
The mission of the ITED is to provide state-of-the-art engineering leadership in order to enable FBI IT to increase mission success and enhance mission capabilities in the critical areas of national security, law enforcement, intelligence, counter-intelligence, and counterterrorism. ITED solutions will ensure accurate and reliable IT capabilities that permit the efficient retrieval, sharing, use, and analysis of information.



CARLO L. LUCCHESI
Assistant Director,
IT Engineering Division

ITMD

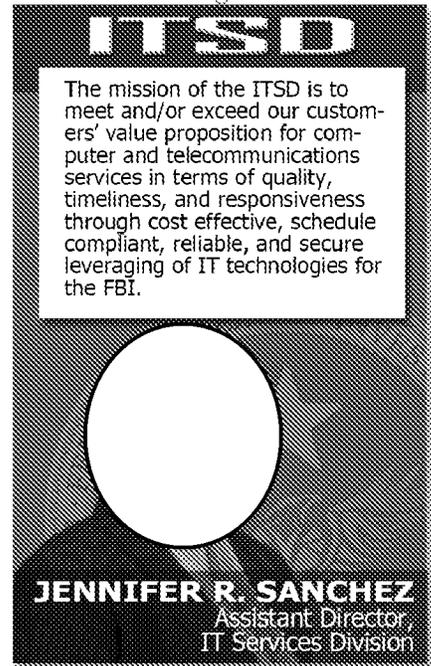
The ITMD will provide leadership and management of IT programs and projects through capital planning, contracts and acquisition, governance, and transition for the effective delivery of IT products and services that meet mission needs through assessments, policy, standardization, and performance metrics.



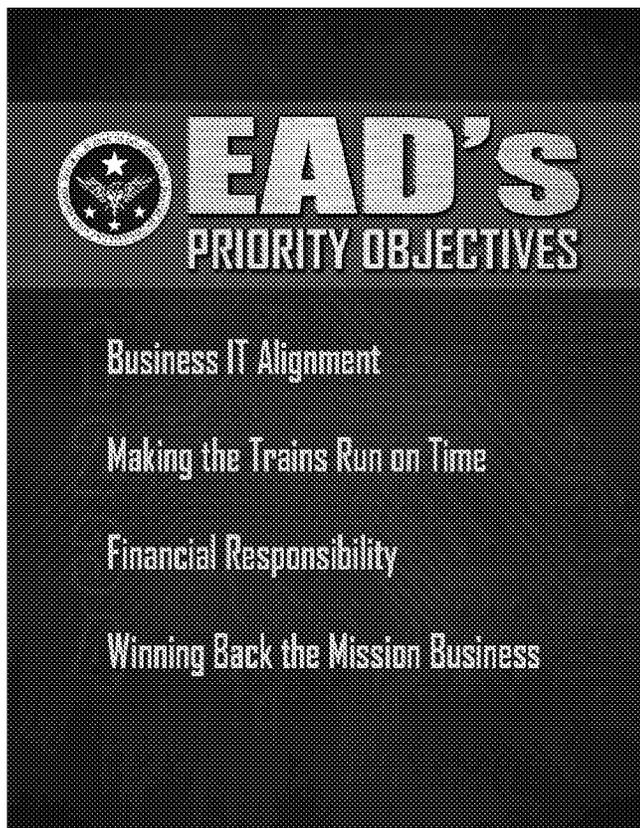
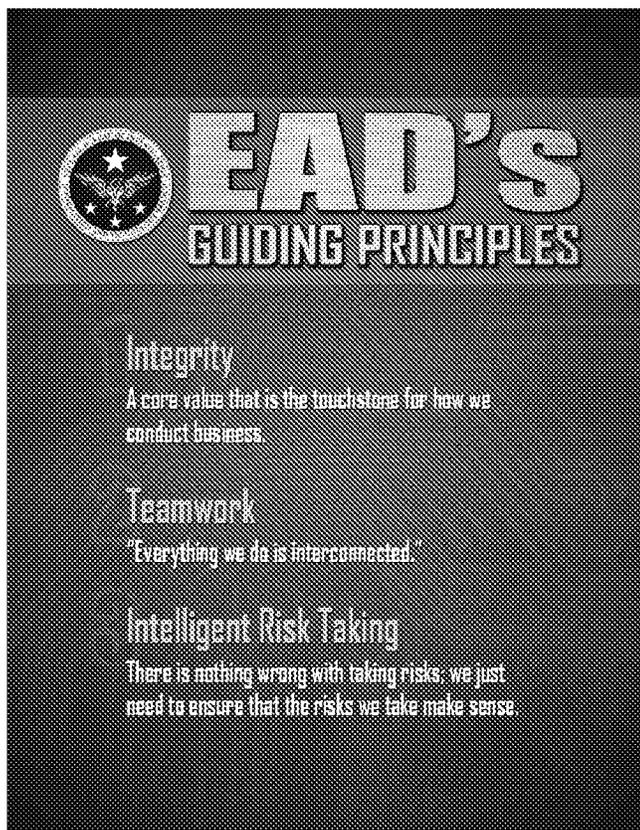
JEFFREY CLEMENT JOHNSON
Assistant Director,
IT Management Division

ITSD

The mission of the ITSD is to meet and/or exceed our customers' value proposition for computer and telecommunications services in terms of quality, timeliness, and responsiveness through cost effective, schedule compliant, reliable, and secure leveraging of IT technologies for the FBI.



JENNIFER R. SANCHEZ
Assistant Director,
IT Services Division



ITB Executive Staff Changes

IT ENGINEERING DIVISION (ITED)

William Searcy III was selected as Deputy Assistant Director and reported from the Operational Technology Division (OTD) on June 16, 2013.

David J. Bukovich, Jr. reported Dec. 16, 2012, to serve as Section Chief, Enterprise Engineering Section.

IT MANAGEMENT DIVISION (ITMD)

Robert Parlato was selected as Section Chief, Executive Staff Section, and reported May 19, 2013.

IT SERVICES DIVISION (ITSD)

Donald L. Kyzar reported March 24, 2013, to serve as Section Chief, Systems Support Section.

Deputy Assistant Director John Hope Retires

Deputy Assistant Director John Martin Hope, a Certified Project Management Professional, retired on June 28, 2013. His colleagues and friends honored him at a retirement ceremony held at FBIHQ on June 17, 2013. FBI executives and managers, former supervisors, and other members of his FBI and ITB colleagues fondly recounted their many memories of working with — and for — him.

Mr. Hope had a long and distinguished career in IT project management with the private and public sectors and the U.S. military. He served as the Chief of Infrastructure and Chief Resource Officer for the Peace Corps where he managed the IT portion of the agency headquarters move and the worldwide migration of computers and networks to a seat management paradigm.

Mr. Hope joined the FBI in 2004. He served as the Deputy Program Management Executive with the Office of IT Program Management until his appointment as Program Management Executive in 2007. Prior to assuming his position as DAD he served as AD of ITMD.

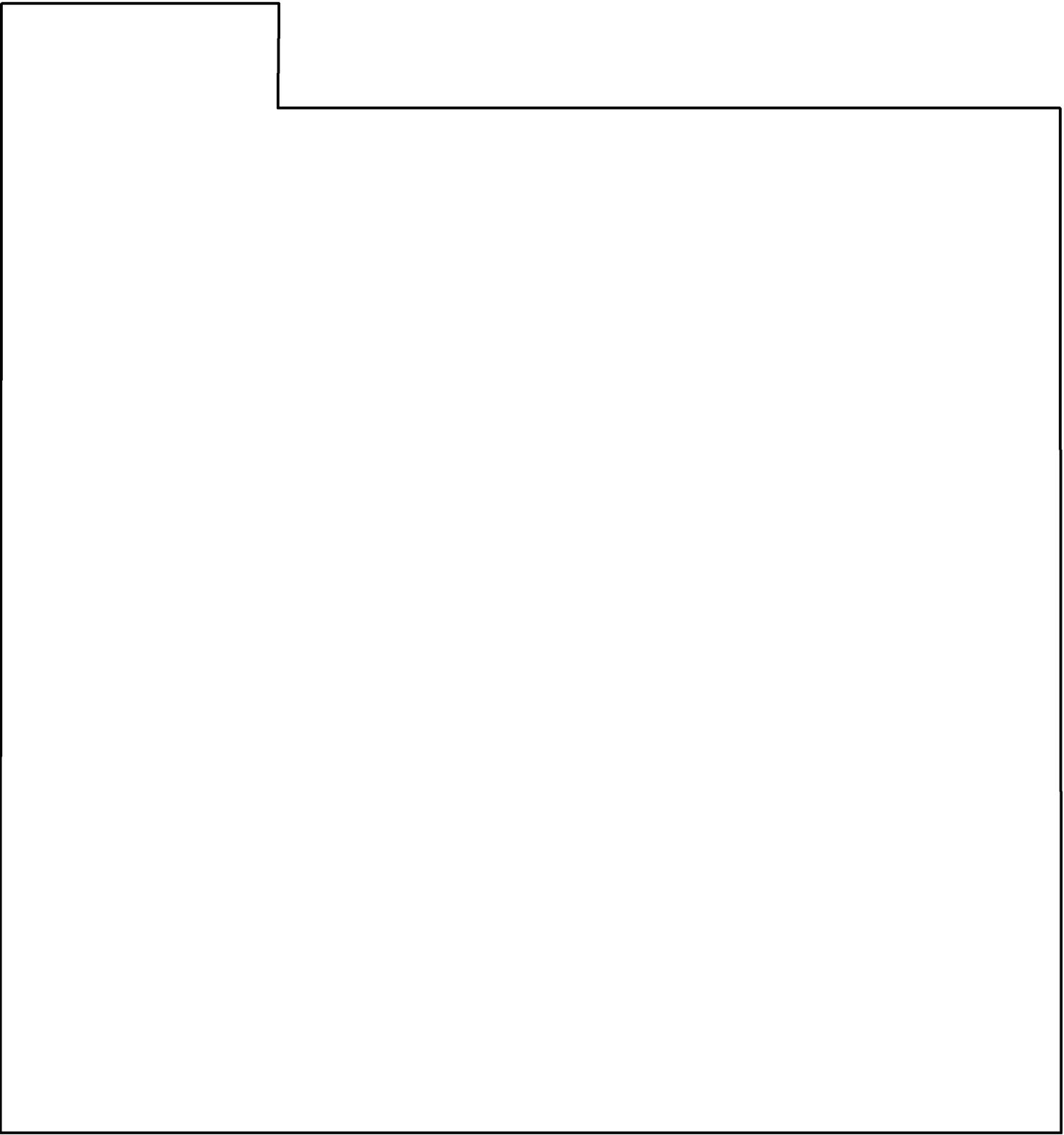
The impact of his tenure with the ITB will be long-lasting, and his leadership style and vision will be missed. ●



Information and Technology Branch Organizational Chart FY 2013



b7E



Strategy Management System (SMS)

The SMS is an FBI-wide initiative led by the FBI Director to actively manage FBI strategy. It provides a formal method for making strategy a part of daily activities and decision making and provides visibility so employees can better understand how their job impacts the direction of the organization.

There are four SMS components:

- **Strategic Shifts** – Describes the strategic changes an organization needs to make in order to achieve its vision
- **FBI Strategy Map** – Shows the strategic objectives necessary for the strategic shifts to be made
- **Performance Measures and Targets (Scorecard)** – Measures inform FBI leadership on progress made toward meeting identified objectives
- **Priority Initiatives** – Projects that are put in place to improve the objectives

During FY 2013, the ITB was actively engaged in the SMS process to pinpoint the strengths and weaknesses of each division and become more efficient at allocating resources.

Executive leadership met with individual units to identify objectives, measures, and initiatives and set up performance metrics for each strategic objective. Out briefings and quarterly reviews provided analysis of the data collected. The ITB uses the SMS to drive its budget; prioritize its work and resources; and provide oversight into executive accountability.

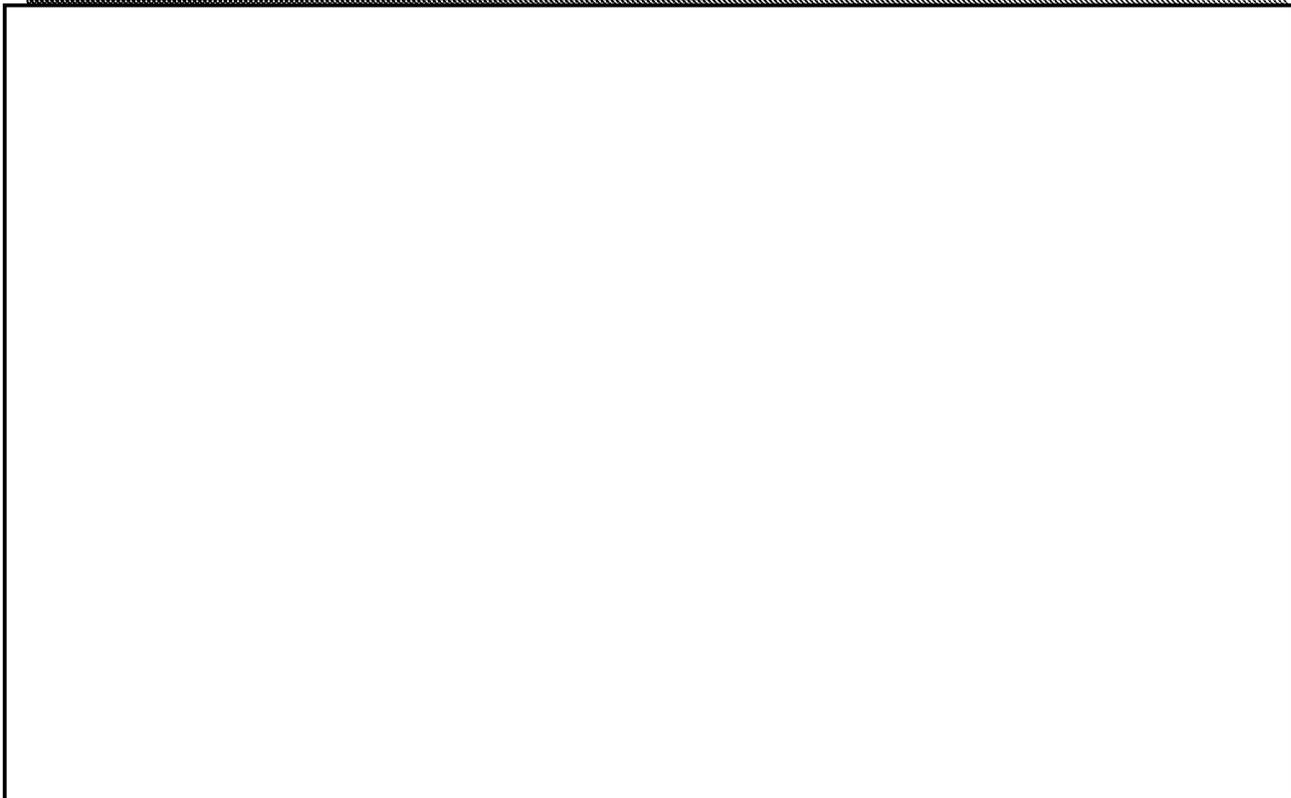
CIO Initiatives

During FY 2013, one of the ITB's challenges was to determine how it could reduce its budget while continuing to provide the expanded array of products and services its customers expected and deserved. A review of each division's top initiatives was conducted including key milestones, risks, resources, and recommendations for implementation.

A decision was made to focus on 12 initiatives for the Branch with an increased emphasis on teamwork, defining ITB divisional roles and responsibilities, and a realignment of personnel resources to work on priority initiatives. Three of the 12 initiatives were also designated as Director's Priority Initiatives.

UNCLASSIFIED//~~FOUO~~

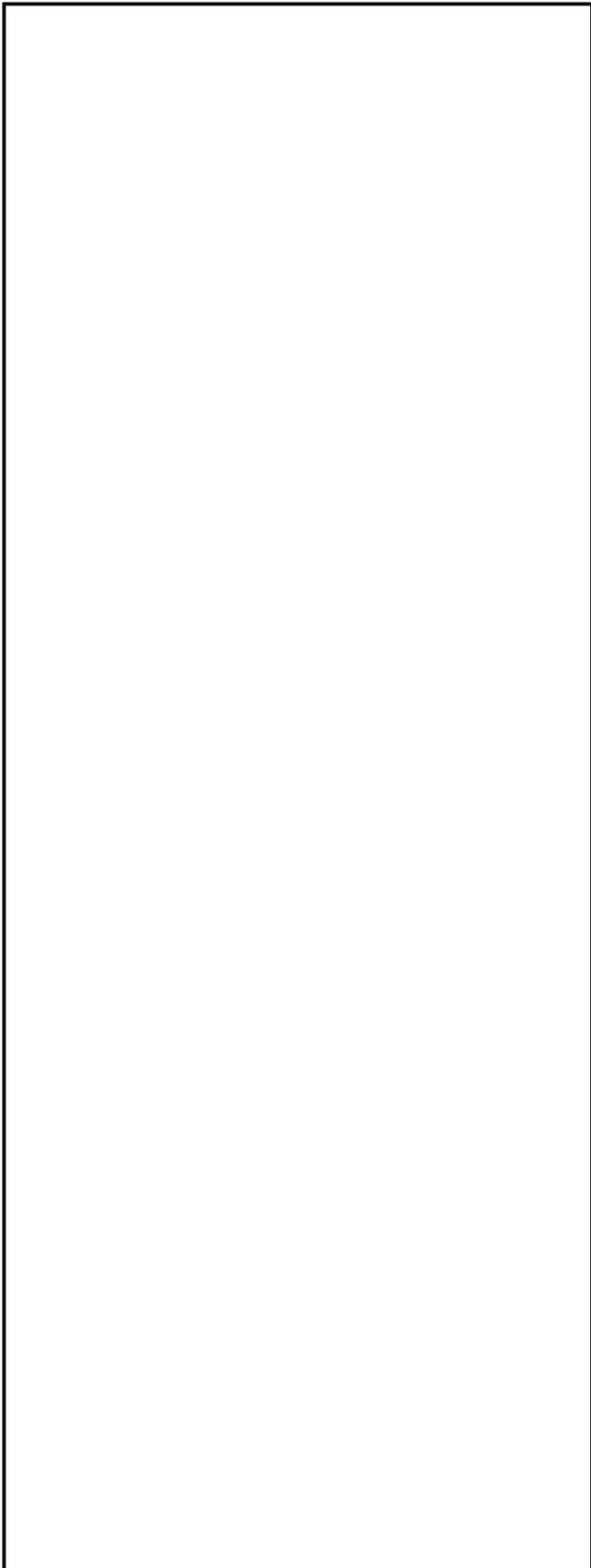
Information and Technology Branch Strategy Map



b7E

UNCLASSIFIED//~~FOUO~~

All 12 initiatives are an integral part of the ITB's mission to provide the FBI the IT support it needs. The initiatives included:



Quarterly IT Business Reviews (QBRs)

One of the EAD's initiatives is to conduct IT QBRs that offer a business perspective on all current ITB initiatives. The QBRs help facilitate communications between ITB's executives and ITB's customers. The QBRs also help the ITB's executives understand the customer's perceptions and expectations of the Branch.

The ITMD Customer Liaison Unit (CLU) serves as the initiative manager for the QBRs. The CLU coordinates with the three divisions to facilitate the production and execution of the quarterly briefs. The CLU staff ensures each briefing includes a portfolio review, a Conditions of Satisfaction graph, a multi-year roadmap, and an IT issues and opportunities report to facilitate the production and execution of the QBRs. The staff also follows up with the executive customers on action items for the following meeting.

This FY the staff delivered a QBR pilot to five executive customers and facilitated 25 QBRs.

Enterprise Data Management Office (EDMO)

The EDMO, housed within the ITED, is responsible for advancing the FBI's enterprise data management initiatives in support of the FBI mission. The EDMO is responsible for guiding the evolution of data management processes and practices to a state where data is more easily discovered, appropriately safeguarded, and more efficiently shared both within the FBI and with partner law enforcement and intelligence agencies.

Enterprise Data Management (EDM) is defined as "a systematic centralized approach to administer the planning and execution of policies, practices, and projects that acquire, control, protect, deliver, and enhance the value of data and information assets."

The EDMO, launched in February 2012, had its charter signed by the EAD/CIO Jerome Pender in February 2013, and is currently supported by a small team of data engineers.

There are many drivers behind EDM:

- ITB Initiative
- [Redacted]
- Webster Commission Report in response to Fort Hood shooting in Texas
- The FBI IT Strategic Plan for 2010-2015
- [Redacted]
- Intelligence Community IT Environment Strategy 2012-2017
- Information-Sharing Environment

With the help of the Enterprise Architecture Program Office and other key partners and stakeholders, the EDMO will develop and implement the FBI data architecture, a Data Reference Model (DRM), a Data Asset Catalog (DAC), an EDM strategic plan, an EDM Maturity Assessment, and an Enterprise Data Access Rules Registry (EDAR).

EDM MATURITY ASSESSMENT

EDMO conducted an organization EDM Maturity Assessment in the summer of 2012 and the fall of 2013 to determine the level of effectiveness of FBI data management practices. EDMO was able to determine, based on maturity level criteria key performance indicator input from various branch points of contact, that there are opportunities to mature EDM practices across the organization.

EDM STRATEGIC PLAN

The FBI EDM Strategy document was developed and circulated to the Office of the Chief Knowledge Officer (OCKO), the ITMD IT Governance Secretariat (ITGS), the OTD, the Criminal Justice Information Services (CJIS) Division, and Cyber Division (CyD) for comments. Comments received were appropriately adjudicated, and the document was circulated for ITED Leadership signature, Chief Knowledge Officer signature, and ITB EAD/CIO signature between June 13 and July 5, 2013.

[Redacted]

DRM -- FBI DATA ARCHITECTURE

As part of the DRM, the EDMO also developed a data abstract model [Redacted] and supports the three Federal Enterprise Architecture (FEA) DRM standardization areas (Data Description, Data Context,

and Data Sharing). Additionally, a Required Artifacts section is being developed to provide users with guidance on developing data management artifacts in accordance with industry leading practices and FBI policy where applicable. Required artifacts include, but are not limited to, Logical Models, Data Dictionaries, and Data Exchange Schemas.

b7E

DAC -- FBI DATA ARCHITECTURE

The DAC is the centralized authoritative resource that tracks all FBI data assets including data sets, associated properties, mission capabilities, and will support links to the EDAR Registry and ITMD Bureau IT Knowledge Repository (BIKR). EDMO developed survey questions to collect data asset specific information that will be stored in the DAC repository database.

EDAR

This joint EDMO-Chief Information Sharing Office effort successfully developed [Redacted] [Redacted] This target was achieved in June 2013.

b7E

Life Cycle Management (LCM)

Emerging projects throughout the FBI necessitate a more enhanced and flexible LCM framework to accommodate unique project needs while maintaining appropriate governance oversight to monitor and guide projects through all lifecycle requirements.

The LCM v6.0, released in March 2013, incorporated an Enterprise Agile Development Framework (EADF) to support the use of various agile development methodologies. The EADF consists of multiple phases that guide project teams through the successful completion of lifecycle requirements relating to a chosen agile development path.

Enterprise IT Governance requirements are aligned with the EADF to support proper oversight of agile development efforts and standardize the information required for review by the investment, project, and technical review working groups, governance staff, and executive leadership. Additionally, the LCM interfaces were enhanced to support the newly designed EADF and existing waterfall methodology.

b7E

The LCM framework v6.1, released on Sept. 3, 2013, expanded the framework for agile software development by incorporating the scrum methodology. This methodology is based on a form of agile project management where self-organizing teams collaborate with the "product owner" to develop a solution and deliver the maximum value to the organization.

Version 6.1 addressed the need for frequent management and customer interaction so that project teams can provide quick and efficient responses to changing customer needs. It also specifies the guidelines, processes, governance requirements, and best practices for system development using the scrum methodology.

Version 6.1 enhances the FBI's ability to:

- Facilitate effective risk management – Open and frequent communication between the customer and cross-functional team members promotes transparency which fosters early identification and management of risks
- Mitigate the potential for rework – Continuous customer involvement and product acceptance throughout the development process leads to a higher quality product
- Accommodate IT projects with varying scope, cost, time, and complexity characteristics
- Offer multiple industry-proven methodologies for projects to use which helps build shared knowledge
- Align and streamline processes to support effective, timely oversight and management of IT projects
- Incorporate best practices from industry and government

Other key updates to the LCM framework include an updated interface to align with modifications, enhancements, increased user functionality, and navigational capabilities.

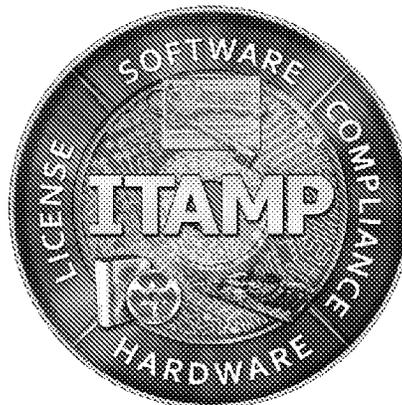
As part of the release of the new version, training is now offered at three distinct levels to provide greater detail for the appropriate audience.

An executive overview is designed for executives and others interested in a general overview. It includes a summary of changes from LCM v6.0 to v6.1; an overview of the FBI scrum methodology; LCM tailoring enhancements; release plans; available training curriculum; and a high-level demonstration of the LCM v6.1 SharePoint site.

Project manager (PM) training is designed for PMs/teams with a solid understanding of agile project management with the scrum methodology. This level offers the same information as the executive overview, but includes an overview of all LCM v6.1 software development methodologies.

Scrum 101 basic training is designed for those with little to no knowledge of, or experience with, agile project

management with the scrum methodology. This level provides interactive detailed training and team-building exercises to demonstrate the concepts and advantages of using the scrum methodology.



IT Asset Management Program (ITAMP)

The ITAMP was created at the beginning of FY 2012 within the ITMD's IT Enterprise Management Section (ITEMS), Capital Planning Unit (CPU). The ITAMP staff performs a host of functions and provides numerous services to their customers. These include managing buying; administering contract compliance; monitoring inventory usage; fostering compliance with policies and standards; and financial and capital planning.

The ITAMP staff currently maintains [redacted]



b7E

FBI's Enterprise IT Governance (EITG) Framework

The EITG framework is the primary means for the FBI to ensure it maintains continuous alignment between its IT investments, associated programs and projects, and its mission priorities. The EITG helps the FBI comply with the requirements of the Clinger-Cohen Act, the Office of Management and Budget (OMB) Circular A-130, and the Government Accountability Office (GAO) IT Management Framework.

The IT Governance Team (ITG) and specifically, the IT Governance Secretariat (ITGS), manages and enforces the EITG framework on behalf of the CIO. Operating as a formal oversight mechanism, the EITG framework regulates the FBI's management of IT investments and related IT efforts throughout the life cycle. The framework ensures that IT investments are prioritized appropriately and IT programs and projects comply with the FBI LCM processes and procedures. In addition, the EITG framework ascertains proper control and monitoring of projects and adherence to project management best practices is maintained. Executive management is apprised of current and accurate information for timely decision making; and corrective actions, if necessary, are pragmatic and swift.

The ITG team members collaborate with the Customer Liaison Officers, the Enterprise Architecture Program Office, program managers, EITG decision authorities, stakeholders and customers, and EITG assessment teams to manage the EITG framework through milestone reviews administered by the enterprise IT Decision Boards.

During FY 2013, IT Governance supported 26 milestone review decisions, performed 12 milestone review assessments, and produced 64 detailed monthly Project

Health Assessments (PHAs) on eight projects. The milestone review assessments are objective independent technical assessments that provide unbiased and actionable information on an IT project's readiness to advance in the LCM process. The detailed PHAs provide insight on the health of each IT project from four perspectives: schedule, cost, scope, and risk.

The ITG Team, Product Assurance Unit, was responsible for



b7E

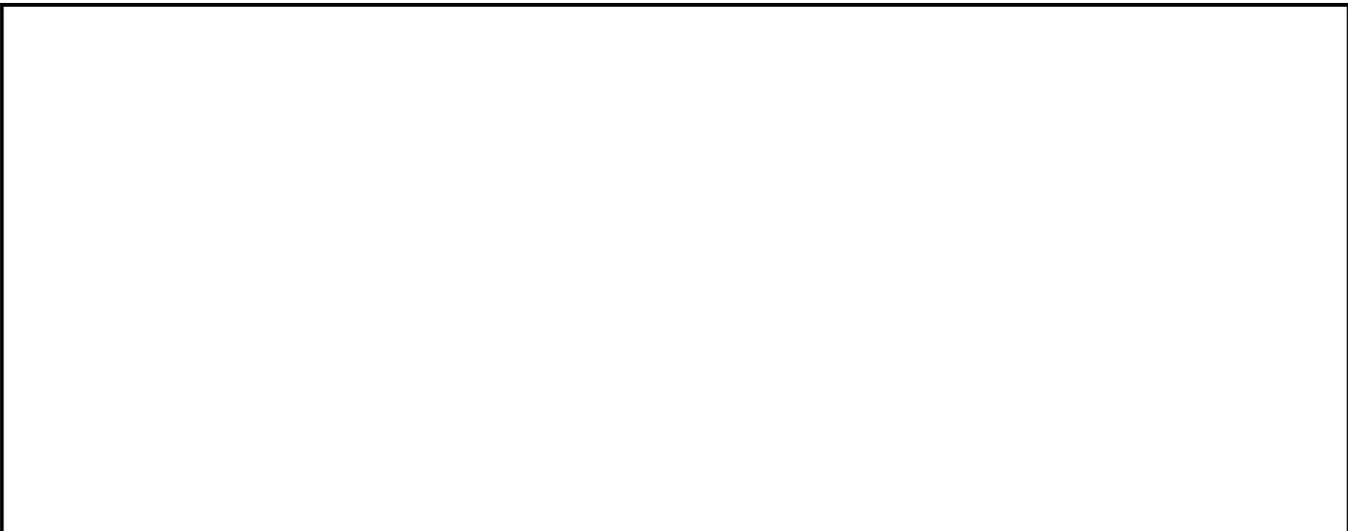
Bureau IT Knowledge Repository (BIKR)

BIKR is an information sharing tool that enables employees to quickly and easily locate and share information about FBI investments, projects, systems, networks, contracts, and processes.

During FY 2013, the BIKR homepage was redesigned to provide a direct interface between the user and the enterprise IT data. The new BIKR homepage is now organized to improve the user browsing experience, with direct access to reports and easier access to branch data.

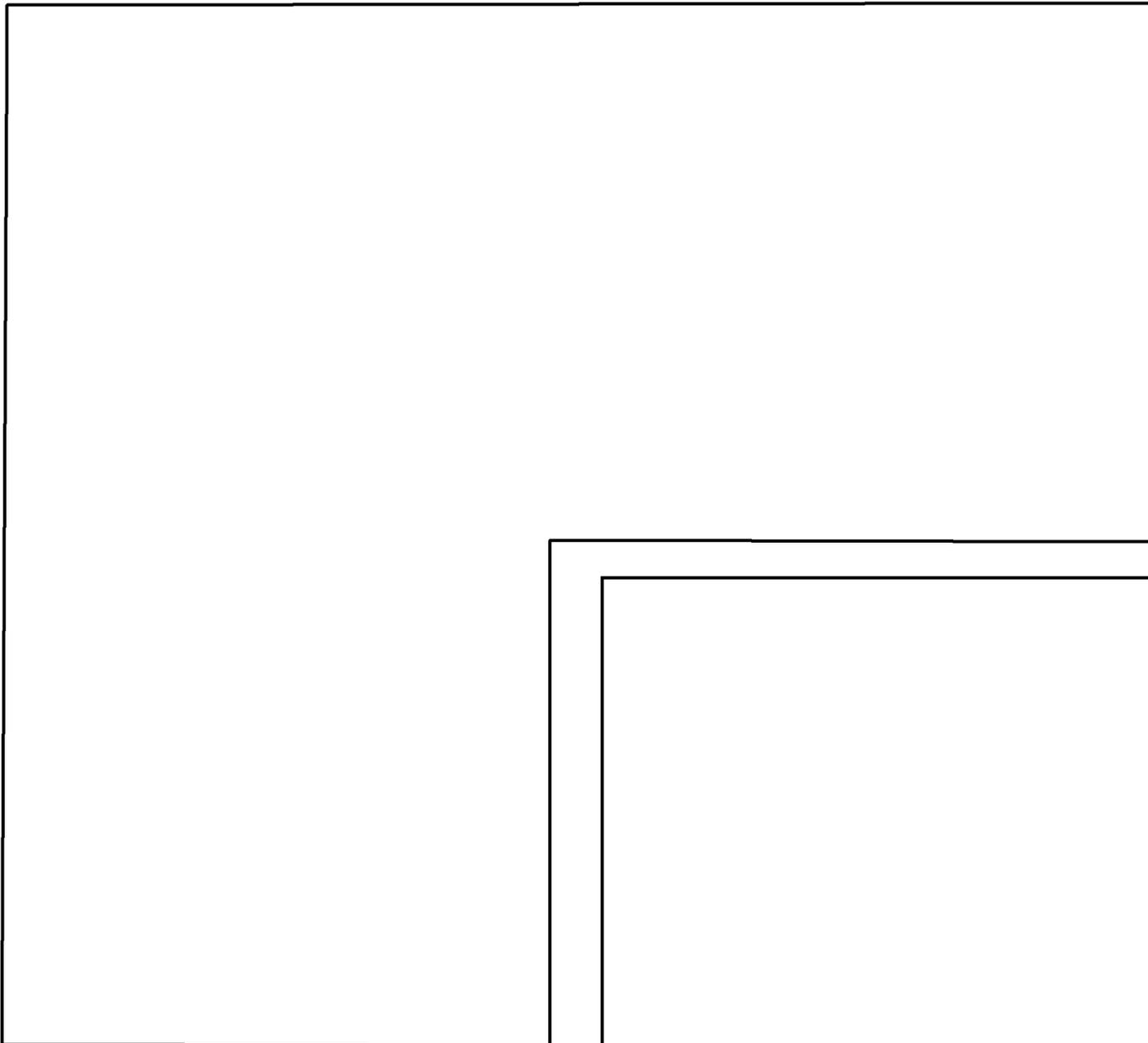
Key changes include a new "Report Hub" section that displays all frequently requested data reports from each functional area and a new "Browse by Branch" section that gives external customers easy access to their data of interest (e.g., IT portfolio summary, IT spending charts).

BIKR has become the authoritative source for information on IT assets. FBI personnel across all branches and divisions use the tool. It has helped employees reduce unnecessary manhours in responding to data calls. ●

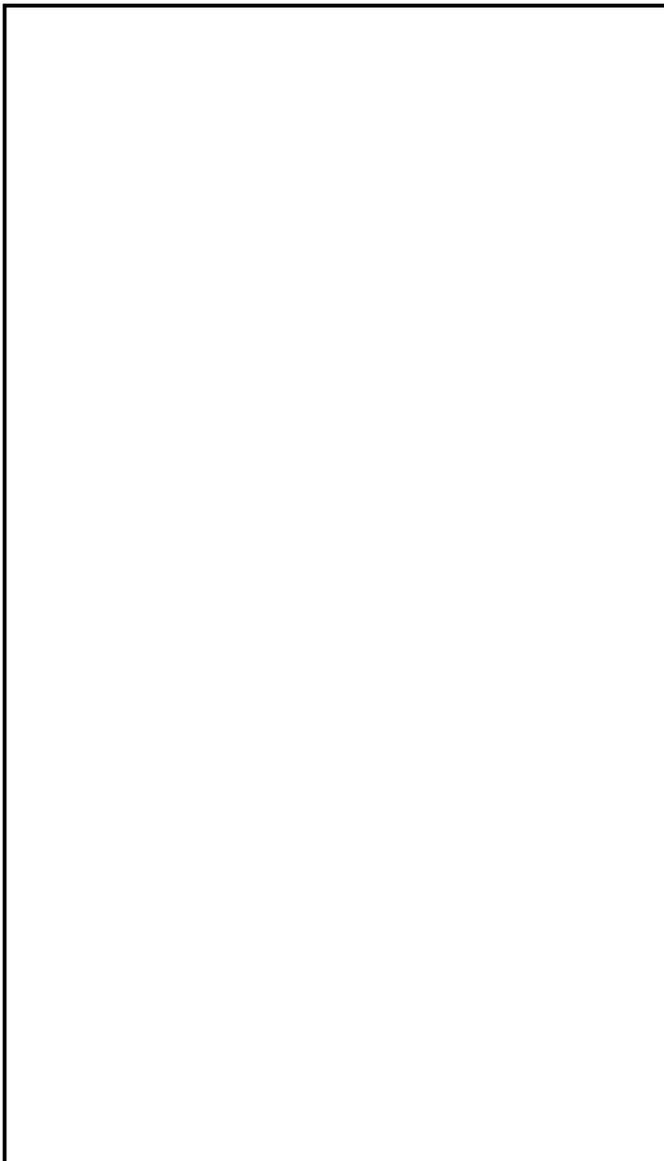


b7E

b7E



b7E



Electronic Laboratory Program (eLAB)

The Electronic Laboratory (eLAB) Program Management Office (PMO) was established in fall 2011, to implement a Laboratory Information Management System (LIMS) in the Laboratory Division (LD). The LIMS will provide electronic visibility directly into evidence tracking and forensic examinations for laboratory personnel.

The eLAB PMO began the process by coordinating with the Facilities and Logistics Services Division



[Redacted]

The [Redacted] upgrade project is [Redacted]
[Redacted]
[Redacted] It
was deployed on Sept. 27, 2013.

[Redacted] replaced 15-year-old hardware infrastructure components that were at the end-of-life and no longer supported by the vendor. The upgraded platform also includes [Redacted]
[Redacted]

The project reflects a well-coordinated effort between the ITMD, ITED, and ITSD. [Redacted] was delivered on time and within budget.

HR Source

HR (Human Resource) Source is a modern web-based Human Capital Management system that incorporates standard processes and best practices from across the Intelligence Community and private sector.

The system enhances technology and business processes and enables the Human Resources Division and customers to quickly secure and report on HR data in a centralized data source.

Core HR Functionality includes Personnel Actions Requests, organization and position management, funded staffing level management, and benefits and payroll documents elections.

HR Source was successfully deployed on Sept 22, 2013.

[Redacted]

[Redacted]

b7E

b7E



National Gang Intelligence Center (NGIC)-Information System

The NGIC is a multi-agency fusion center that serves as a central intelligence resource for gang information and analytical support. It supports Federal, state, local and tribal law enforcement partners with timely and accurate information sharing and strategic/tactical analysis of information focusing on the growth, migration, criminal activity, and association of gangs that pose a significant threat to communities throughout the United States. The Center is staffed by gang experts from the following agencies:

- FBI
- Drug Enforcement Agency
- Bureau of Alcohol, Tobacco, and Firearms
- Immigration and Customs Enforcement
- Customs and Border Protection
- Department of Defense
- U.S. Bureau of Prisons
- U.S. Marshals Service
- National Drug Intelligence Center

The NGIC must be able to effectively and efficiently share intelligence on gangs with its law enforcement partners and perform strategic/tactical analysis on the available information.

The NGIC and the Investigative Projects Unit have worked together to develop

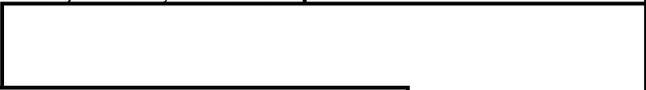


The system was deployed to internal users in January 2011 and to external users in March 2011. Phase IV was completed on Aug. 31, 2013. The project's transition to CJIS is scheduled for February 2014.

Next Generation Name Check Program (NGNCP)

The NGNCP supports the mission of the FBI to protect and defend the United States against terrorist and foreign intelligence threats

b7E



The program provides information from FBI files in response to name check requests received from a variety of federal agencies.

When complete, NGNCP will provide secure user interface services, automated workflow services, and system interface services, which will provide the NGNCP the capability to:



b7E

The NGNCP is sponsored by the Records Management Division (RMD) with IT program management provided by the ITMD.

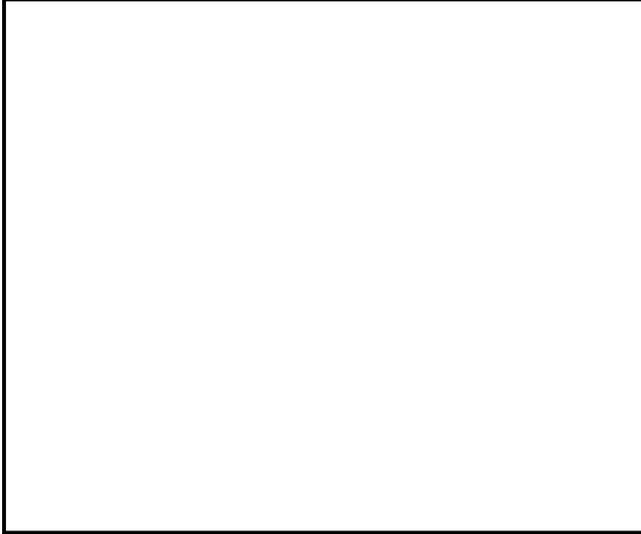
The ITMD initiated the final requirements review in November 2012. After various reviews and development checks, Release 1 of the NGNCP was completed on Sept. 10, 2013. Deployment is scheduled before the end of calendar year 2013.

Sentinel

Since its debut as the FBI's electronic case management system in July 2012, more than 20,000 employees use Sentinel on a daily basis to create new investigative cases, write electronic communications, and search documents to share information, request assistance, etc.

After passing its one-year anniversary mark, three major releases, adding additional enhancements to the system, were deployed in FY 2013. In each release, the Sentinel Team collaborated with other FBI Divisions to improve or expand on existing functionalities and capabilities or to develop new ones, allowing the system to mature.

In November 2012, the Sentinel team partnered with the CJIS to release (1.2) the first set of system enhancements



The second major release (1.3) of Sentinel in February 2013 was the addition of

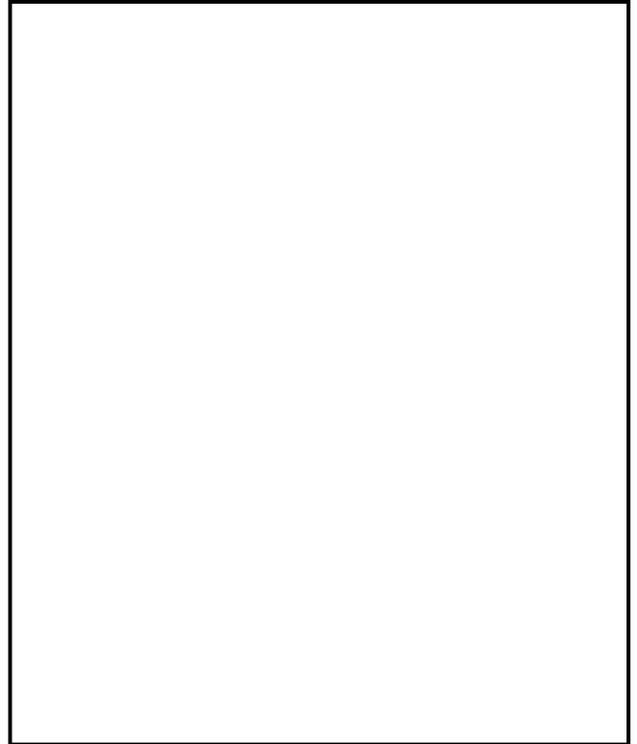


In collaboration with the Cyber Division (CyD), the Sentinel team improved and expanded Sentinel's functionalities and capabilities with a new release (1.4) deployed in September 2013. This was the largest collection of enhancements released by the Sentinel team since the system's initial launch. Besides a more functional and intuitive experience for Sentinel users, this release included improvement



b7E

Other enhanced capabilities included:



As with each new release under development, the Sentinel team continues to incorporate user feedback to integrate the latest technologies to deliver capabilities satisfying users' operational needs.

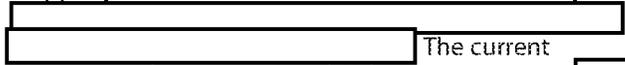
The next major release (1.5) is tentatively scheduled for deployment in FY 2014. It will include



b7E

SharePoint 2010 Migration

The ITSD, Web Services Support Unit (WSSU), provides support



The current Enterprise SharePoint Farm (ESF) is on a SharePoint platform which will be upgraded to SharePoint. The migration effort impacts all applications and websites hosted on the ESF.

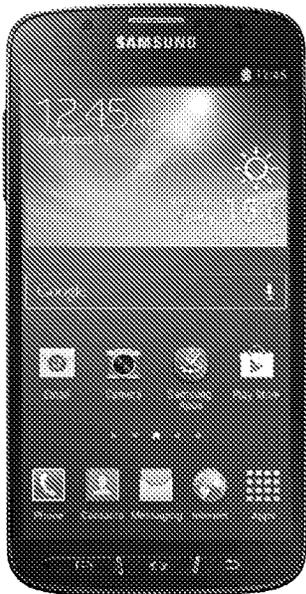
This upgrade provides the customer with greater capabilities and functionality, advanced records and document management, a scalable platform, more robust search capabilities, and a better customer experience that is seamless and familiar to the Microsoft Office interface.

Deployment will be accomplished in phases. The first phase began in June 2012.

The WSSU decommissioned the legacy SharePoint environment in May 2013. All custom SharePoint applications were migrated to SharePoint by May 2013.

Smartphone - Mobility

The Samsung Galaxy S4®, a 4G Android device, was selected as the FBI's next smartphone to replace the current BlackBerry device in June 2013. The decision to move from the historical FBI use of the BlackBerry device was based on the need for a solution that met the vast needs of employees who rely on mobile communications to complete their various missions.



The Android device will leverage advanced mobile technologies and applications without compromising security and compliance. It is a part of the Samsung for Enterprise, SAFE™, family and offers many outstanding features and capabilities including: Touch screen; a multi-tasking capability called multi-window; and an instant preview of photos, files, links, and text without touching the screen with Air View™.

The FBI will also be implementing a new mobile device management platform to accommodate the new phone.

The ITB is coordinating with the FD, SecD, and CJIS to ensure a smooth transition of the smartphones throughout the enterprise. Teams of ITB employees will be mobilized during scheduled deployment dates and will be onsite to assist Field Office (FO) Information Technology Specialists (ITs) with issuing and activating the devices.

Deployment is tentatively scheduled to begin in January 2014 with the FOs being the first recipients. Currently, ITB has a small pilot of 180 users to include senior executives, agents, and professional staff across various FOs and HQ divisions.

Microsoft® Windows®7 Operating System

Microsoft has announced that the company will cease support for its product, Windows XP, in April 2014. This would include the cessation of all updates, to include critical security patches. Therefore, the FBI is in the process of transitioning all desktops to the Windows 7 Operating System baseline.

Benefits include:

- Quicker computing with decreased "boot up" time (30 percent faster)
- More efficient use of computing resources
- Increased speed, significant performance, usability, security, enterprise integration, and internal technology improvements
- Ability to run system programs and background services when needed, so computer's resources are available when most needed
- A cleaner, crisper, more modern look
- Virtual file libraries which allow users to group and search files quickly
- Ability to "pin" a program to the taskbar so that it is only a click away
- Ability to hover over an item and view a thumbnail preview of open documents
- Ability to preview two documents side-by-side using the Aero Snap function
- An environment which allows geospatial, graphical, and data intensive applications to run faster and more effectively

The ITED conducted engineering pilots on FBI Net and UNET within the ITB from April 1, 2013 to June 28, 2013. The ITSD conducted a business pilot from June 17, 2013, to Aug. 31, 2013, in the Dallas, Denver, Little Rock, Louisville, and Tampa Divisions. The Enterprise deployment began on Oct. 1, 2013, with a total of 36,789 Windows 7 workstations migrated since Oct. 1, 2013.

SCINet Windows 7 upgrade for FOs was completed on Aug. 16, 2013 and the SCINet Windows 7 upgrade for FBIHQ was completed on Sept. 30, 2013.

Unified Financial Management System (UFMS)

On Sept. 29, 2013, the IT Program Management Section project managers delivered the UFMS, a Department of Justice (DoJ)-wide effort to implement a single financial system, to the FD, making the UFMS the single financial system of record for the FBI. It replaced a collection of financial tools that were no longer compliant or capable of managing the FBI's finances.

Delivery of the system involved all parts of ITB (as well as the FD, Resource Planning Office, and others). The ITB provided program management, core IT infrastructure, and software development best practices. Full implementation of UFMS included nationwide training of more than 2,800 users filling a dozen role-based class formats as well as the facilitation of the nationwide deployment of check scanners to every FO.

When fully deployed on Oct. 7, 2013, the UFMS will enable the FBI to more effectively manage financial resources in support of its mission by replacing the 30-year-old Financial Management System (FMS) and the disparate collection of tools developed over time to augment it. The UFMS will streamline business processes, provide consolidated management information, and support compliance with Federal accounting regulations.

The UFMS will interface with more than 35 systems, both internal and external to the DoJ and FBI (e.g. Sentinel, Enterprise Process Automation System, and the U.S. Department of the Treasury). ●

Centralized Tiered Storage (CTS)

There is a greater need now more than ever to identify a solution to the FBI's data storage problem as unstructured data continues to increase as much as 25 percent annually with no end in sight. Experts in network computing say that nearly 90 percent of today's data has been generated in the past two years. This proliferation of data is creating challenges for IT professionals responsible for storing and managing all that data.

The CTS project, managed by the Storage Management Support Unit (SMSU), Infrastructure Support Section, ITSD, was started in November 2012. It was completed one month ahead of schedule in August 2013.

The CTS solution provides a centralized and virtual platform across the FBI's secret enclave FBI Net for application hosting, file storage, and consolidated management for all FOs and Resident Agencies (RAs). This project updates and simplifies the infrastructure for 126 continental U.S. sites as defined by the Next

Generation Workspace Project. The updated systems provide central storage for FOs and RAs at Site 73 and at the CJIS Division.

The SMSU deployed [redacted] to each FO and RA, replacing traditional file servers on FBI Net. The implementation of [redacted] increases storage capacity up to five times the current amount and ensures the availability of the data if it becomes inaccessible or is lost due to a disaster situation. [redacted]

b7E

The cost savings for implementing this initiative are also beneficial as it reduces overall maintenance and tape back-up activities by allowing local ITs the opportunity to focus on other IT concerns. With the deployment of CTS, the SMSU eliminated the need for 188 file servers that were located at 116 sites across the U.S.

Besides storage management and file backup, the CTS solution provides replication of the FBI's data at multiple sites. This new capability ensures consistency between redundant resources and improves reliability and accessibility. Information is captured on a regular basis using an innovative feature called "snapshots." These snapshots are point-in-time copies of data files. All of the data from any FO is replicated at two different sites. This built-in redundancy is critical for data contingency operations.

The CTS was a significant accomplishment for the FBI and was recognized by Information Week Magazine as one of the Top Ten Government Innovators for 2013.

Enterprise Circuit Consolidation (ECC) Network Consolidation Efforts

The ECC initiative is an ITB effort to collectively streamline and reduce telecommunications infrastructure support costs across the FBI enterprise. The ECC is an ongoing endeavor that involves multiple cost-avoidance strategies including:

- Analyzing circuit billing overcharging and errors
- Turning off unused circuits
- Limiting new--and converging--stand-alone networks and enclaves
- Minimizing telecommunications infrastructures and footprints
- Optimizing bandwidth utilization
- Re-engineering outdated technologies
- Eliminating excess spending on the FBI's communications infrastructures

The ECC also provides direct engineering support on several ongoing initiatives such as the DCSNet and BlackNet FBI-shared services effort and the Federal Data Center Consolidation Initiative.

Many FY 2013 initiatives have already been realized or are in their final phase of cost reduction monitoring. The ITED's ECC team identifies a cost-saving strategy; recommends implementation; briefs the strategy to ITSD for implementation; and reviews the monthly billing statements to validate the recovery of those cost-avoidance strategies.

FY 2013 cost-avoidance strategies have resulted in a cost avoidance of \$1.27M with additional cost avoidance to be realized in FY 2014.

Enclave Consolidation Initiative (ECI)

The ECI is an initiative to allow the accessing of multiple network enclaves from a single user workstation using a trusted thin-client technology and Secret and Below Interoperability certified cross-domain product.

The ECI provides an opportunity to remove 80 percent of the current unclassified network infrastructure and eliminates the need to refresh all UNet workstations. The ECI reduces FBI network infrastructure complexity, improves UNet service performance, and achieves substantial cost avoidance by eliminating an upgrade of UNet hardware and printers and the need to refresh the workstations. The ECI also extends UNet access to offices and facilities that are currently lacking this capability.

Phase 1 from Sept. 5 to Oct. 30, 2013, included a 50-user engineering proto-pilot conducted at select sites. The proto-pilot included online user surveys to determine what adjustments were needed.

The ECI Phase 1 pilot received positive user feedback and was well received by FO and HQ ITSs due to its rapid software deployment and ease of use. The ECI is depending on hardware technical refresh funding to deliver the capability to the enterprise. It is part of the ITB's SMS initiative, "Implementing End User Environment," deliverable for FY 2014.

Phase 2 will have an expanded engineering pilot that will increase the ECI component to 10,000 users with current hardware technical refresh funding in FY 2014.

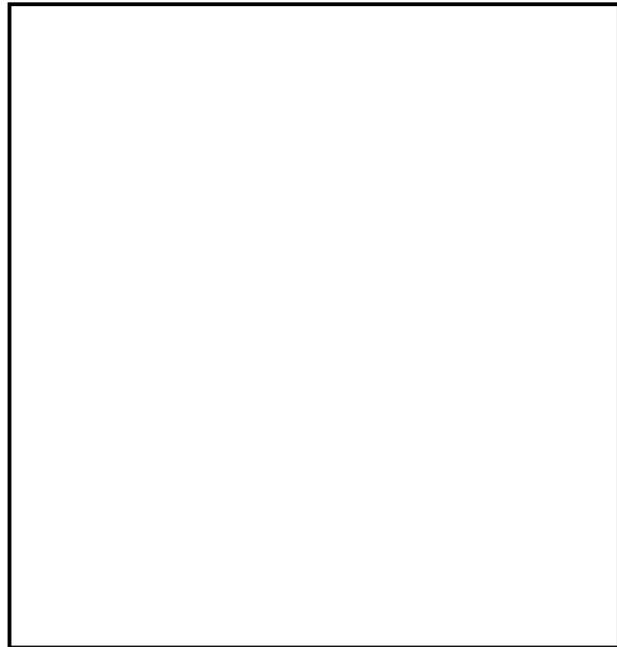
Deployment to the entire FBI enterprise during phase 3.1 is scheduled to take place in FY 2015.

Enterprise Remote Access Service (ERAS)

The ERAS provides users with secure access to FBINet and UNet virtual workstations over any Internet connection.

[REDACTED]

the ERAS ultimately supports mission-critical efforts, complies with the COOP policy, and affords telework capability for all FBI users.



The ERAS received an Authority to Test from the SecD to be deployed in a limited pilot. [REDACTED]

This capability has the potential to transform the FBI organization into a mobile workforce that can achieve results more effectively and efficiently. The ERAS concept can also be applied to a wired environment at larger sites to collapse enclaves; reduce the physical footprint of user equipment; decrease the overall power and cooling consumption; and reduce operations and management support.

Printer Refresh

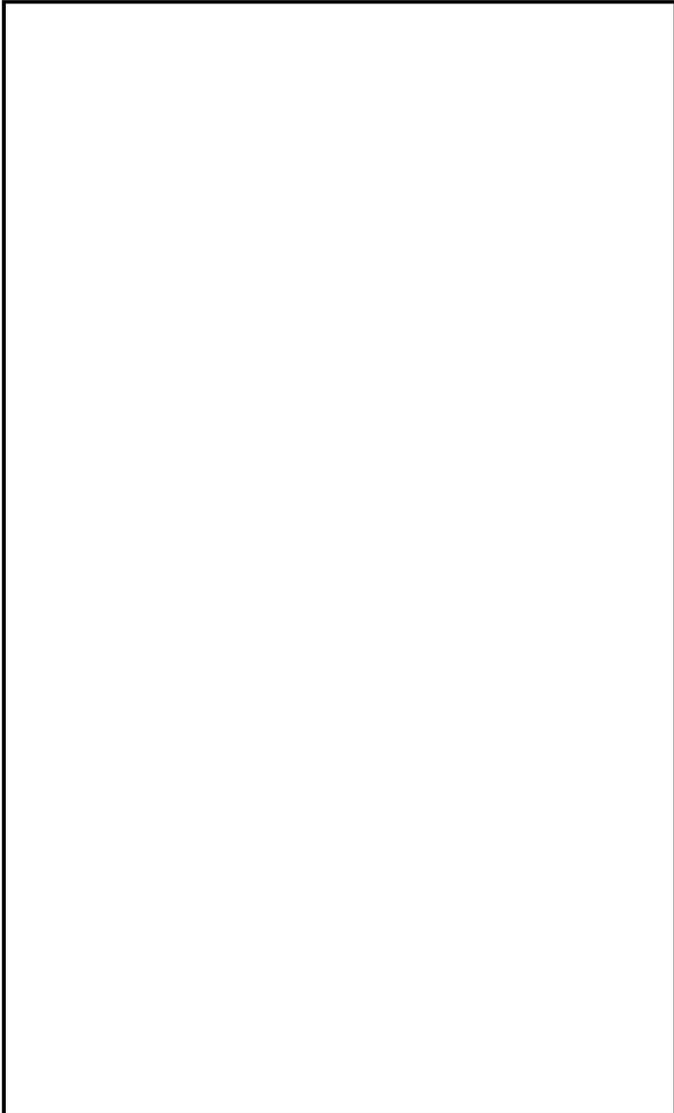
The Multi-Function Printer (MFP) and deployment project was a joint venture between the ITSD and the FD to refresh and standardize printer models on FBINet. Having standardized printers allows the IT staff to provide better support services. The MFPs offer traditional printer capabilities as well as enhanced functionalities such as copying and scanning.

The Regional IT Program Managers, who are embedded in the field, the FO ITSs, and others across ITSD worked collaboratively to coordinate the intricate logistics of the MFP and Single-Function Printer (SFP) deployment. This was the first major deployment for the program managers since they assumed their positions.

This effort included:

- Identifying the FO's equipment needs and managing the shipping and installation of MFP servers, which included facilitating and tracking server installations and identifying and addressing additional network requirements.
- Coordinating shipping/delivery information to approximately 130 different sites.
- Verifying shipment delivery and receipt, which included addressing equipment issues (e.g., missing peripherals, damaged equipment).
- Facilitating the installation and troubleshooting of the MFPs and SFPs which included:
 - Providing training for the installation and set up of the MFPs and SFPs (via Microsoft meeting/webcam)
 - Ensuring IT personnel had the necessary overtime and TDY assistance to successfully install their allotted MFPs and SFPs
 - Ensuring IT personnel obtained the necessary technical support needed to successfully install their MFPs and SFPs

As a result of their collaborative efforts, a total of 2,444 MFPs and SFPs were successfully delivered to the field between August 2012 and December 2012. Installation is scheduled to be completed by December 2013.



b7E

NGSCION Deployment

The deployment of Next Generation Sensitive Compartmented Information Operational Network (NGSCION), the FBI's upgraded Top Secret/Sensitive Compartmented Information (TS/SCI) network, was completed in March 2013. The NGSCION deployment was a collaborative effort between the ITB, SecD, Facilities and Logistics Services Division, the executive sponsor, the NSB, and all field divisions.

NGSCION was deployed to all FBIHQ divisions, 56 FOs and more than 120 RAs and 20 Legats, for a total of more than 10,000 users. The successful deployment of NGSCION was a significant milestone [REDACTED]

Customers now have reliable equipment to use.

During May 2013 the TS/SCI enclave was renamed SCINet to be consistent with other FBI networks.

Classification Management Tool (CMT)

The ODNI-mandated [REDACTED] [REDACTED] CMT applies classification markings to electronic documents and email. The CMT is a standard tool currently in use throughout the Intelligence Community (IC). It allows employees to automatically select the correct classification criteria based on the information being classified.

b7E

The CMT allows for the proper classification marking of FBINet and SCINet email, as well as other Office documents such as Excel spreadsheets, PowerPoint slides, and Word documents. Versions 2.7 and 3.1 have been implemented on FBINet and SCINet.

The CMT 2013 is currently in business pilot, is installed on approximately 5,000 workstations on FBINet and 3,000 workstations on SCINet. The ITB plans for desktop

enterprise deployment of the software to be completed by the end of December 2013.

The CMT is also a component of Sentinel and Guardian. Both of those systems are currently working to implement CMT 2013 within their systems and will be updating according to their own internal update schedules.

The new CMT 2013 for Outlook Web Access was piloted on FBI Net and SCINet. [redacted]

[redacted] This is a new tool that has not seen enterprise deployment anywhere in the IC, with the FBI helping to shape its development.

e-Discovery

The FBI is subject to certain unique retention and disclosure requirements with respect to email. The FBI is required by the Federal Rules of Civil Procedure as well as Criminal Procedure, to preserve and produce ESI that is relevant to litigation.

The ITB is partnering with the OGC, RMD, SecD, Inspection Division, and the FD to launch new e-Discovery tools and processes and centralize all ESI search and collections.

In October 2012, the e-Discovery team completed the migration of over 159 million FBI Net emails from September 2009 to July 2011, to the new Symantec Enterprise Vault, in support of OGC's litigation hold requirements. This was performed using an email migration tool.

The e-Discovery Program Management Office team is also currently working with the ITED, ITSD, RMD, and the Sentinel team to develop and deploy a Records Marking Tool (RMT) within Outlook that will be piloted and deployed across the enterprise. The RMT will allow users to designate email as a non-transitory record, non-record, or transitory record.

The RMT deployment occurred in phases with initial pilots beginning in December 2012 and phased deployment to the enterprise beginning in March 2013. At the end of FY 2013, a RMT had been successfully deployed to more than 35,000 users, with the remainder scheduled to be completed in FY 2014.

Facility Security System (FSS)

The FSS is considered a critical application to the FBI's operations. [redacted]

[redacted]

[redacted]

A re-engineering of the FSS was needed to comply with the Office of Inspections, Inspector's Report "An Audit of Contractor Administrative Controls." This provided an opportunity to re-engineer the legacy mainframe version of FSS to a web-based application.

The Human Resources Applications Support Unit met extensively with SecD personnel from numerous units to gather requirements. At the same time, SecD personnel re-evaluated several of their business processes to improve the clearance process.

The new FSS was launched on Aug. 19, 2013. [redacted]

[redacted]

Provisioning and Access Control (PAC)

The PAC system provides the FBI with improved enterprise wide IT security management by controlling users' access to information, applications, and services. With better identity and access management procedures in place, the FBI benefits by improved operational efficiencies, reduced costs, compliance with government regulations, and mitigation of risks.

In FY 2013, the ITED delivered the first of PAC's functionalities-- [redacted]

[redacted]

In May 2013, ITED developed a second system functionality which automated and streamlined several manual tasks [redacted]

[redacted]. Final testing of this functionality and transition to the ITSD will occur next fiscal year.

In September 2013, PAC replaced the Enterprise Directory Services interface within Sentinel. [redacted]

[redacted] PAC is currently the source for Sentinel's data attributes.



virtualized, and reliable PKI infrastructure was established that removed antiquated equipment and eliminated all single points of failure by adding redundancies, resulting in a more robust system.

b7E



Lastly, the ITED established an Operations and Maintenance contract with ITSD to support the PAC system and formed an agreement for out-year funding with the ITSD to ensure PAC functionality could be sustained over the life span of the application.

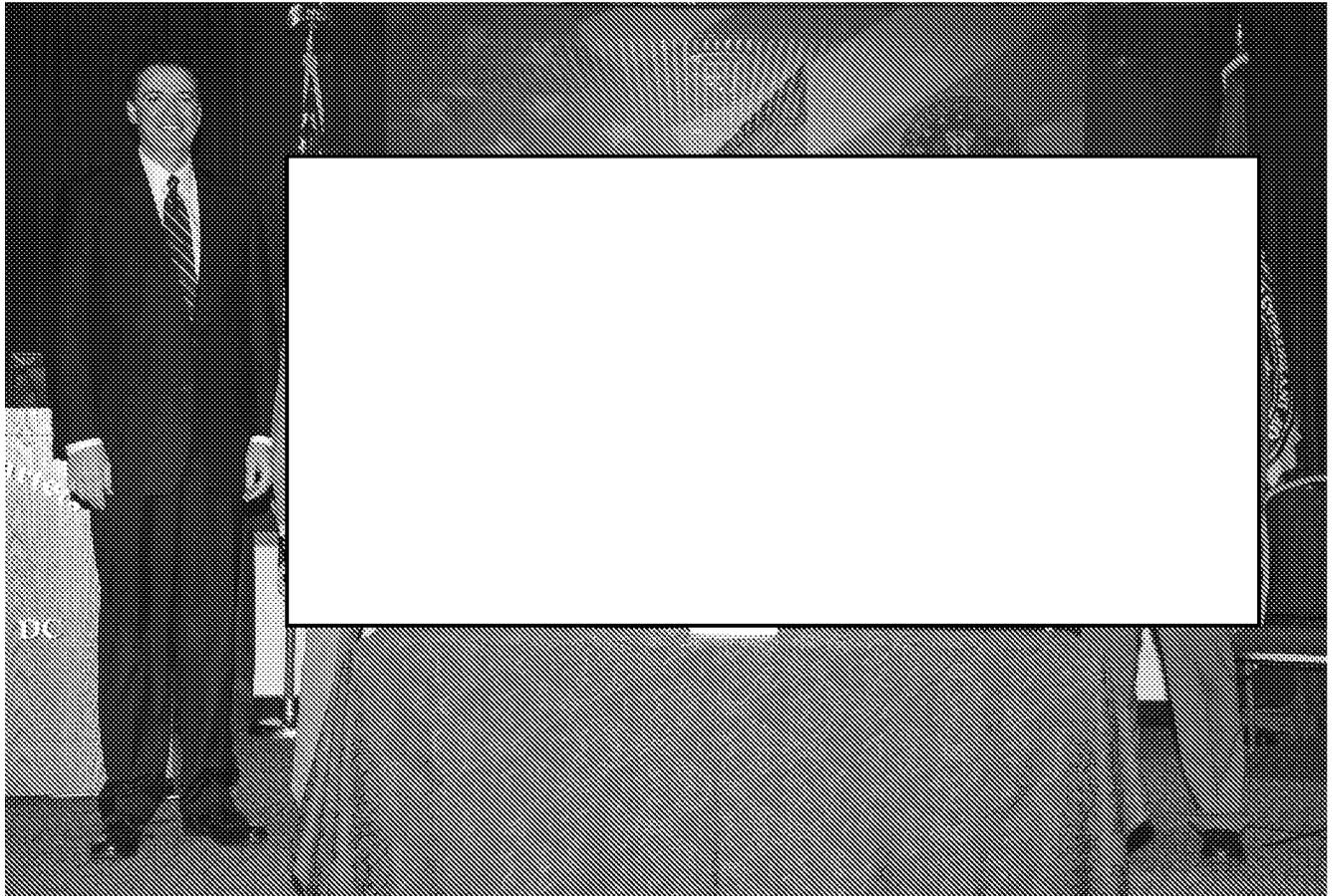
In addition, the new infrastructure will allow for easier and faster failover capabilities by utilizing products designed for high system availability. This enhanced dependability improves the ability to support mission critical applications such as Sentine. The deployment of the PKI virtualized infrastructure will reduce costs because of increased manageability and decreased travel time to and from the data centers. Cost savings will also be realized due to the consolidation of physical hardware.

b7E

Public Key Infrastructure Virtualization (PKI)

The PKI refresh project is a major ITSD initiative. A newer,

The PKI virtualization was successfully deployed on Sept. 30, 2013, at the production site with limited interruptions to the FBI user community.



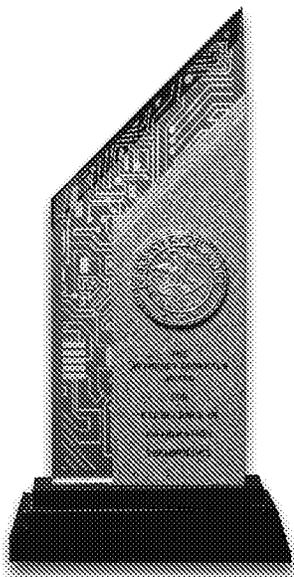
b6
b7C

Attorney General's Award recipients

Attorney General's Award

EXCELLENCE IN INFORMATION TECHNOLOGY

Superior Program Management of Sentinel Case Management System



In late 2010, the ITB Sentinel Agile Team assumed responsibility for Sentinel program development. Over a period of 22 months, the Sentinel team exercised innovation while including customers in the development cycle. Using a much smaller group of specialized developers consisting of FBI agents, professional support, and subject matter experts from specific technology providers, the system was completed in less than two years, within the original budget, and meeting all functionality requirements.

The quality and punctuality of the team's development and implementation ensured a smooth transition for all FBI employees. The team invested in training opportunities for employees and deployed extensive online training materials.

The Sentinel project was fully implemented in July 2012 and became the FBI's case management system of record including such advanced components as electronic signature, workflow, advanced search, and records management capabilities. Sentinel's efficiency gives the FBI and its workforce more time to collaborate with its partners, investigate issues, and protects the U. S. and its interests.

ATTORNEY GENERAL'S AWARD RECIPIENTS

- Assistant Section Chief [redacted] ITSD
- Unit Chief [redacted] ITMD
- Special Assistant [redacted] ITMD
- Supervisory IT Specialist [redacted] ITED
- IT Specialist [redacted] ITED
- IT Specialist [redacted] ITED
- Supervisory Special Agent [redacted] ITED
- Supervisory Special Agent [redacted]
Counterterrorism Division
- Supervisory Special Agent [redacted] Los Angeles FO
- Special Agent [redacted] Las Vegas FO
- Special Agent [redacted] Denver FO
- Special Agent [redacted] Denver FO
- Special Agent [redacted] Charlotte FO
- Special Agent [redacted] Sacramento FO
- Supervisory Intelligence Analyst [redacted]
Directorate of Intelligence

Director's 2013 Annual Awards

AWARD CATEGORY: EXCELLENCE IN PROGRAM MANAGEMENT

[redacted] (ITMD)

The Asset Management System (AMS) project team successfully developed and implemented the FBI's consolidated Asset Management System. As Infrastructure Lead, [redacted] developed and provided strategic guidance on all technical infrastructure aspects of the AMS project. He also identified the necessary technical activities required for the project and monitored the vendor's technical delivery. His efforts in maintaining regular and routine communication channels between ITB components, the FD, his project team, and the vendor's technical team were a major element in the success of the project.

[redacted] (ITMD)

[redacted] was one of three primary functional subject matter experts for the AMS project. In this role, she represented and supported the project and the FD by providing insight into current business processes and legacy system business logic. Each expert played a significant role in reconciling asset management data and in determining data-mapping activities and strategies for "to-be" business processes. More recently the group led training activities in multiple FOs and Quantico, while continuing to provide agents and supply technicians with expert advice. There were many new technical challenges with the development and integration into the FBI environment because this was

b6
b7C

the first time this COTS solution had been deployed within a technical environment similar to the FBI's. The AMS team worked 12–14 hour days and weekends for consecutive months to overcome challenges and develop solutions. The AMS was officially launched throughout the FBI on Oct. 9, 2012.

AWARD CATEGORY: OUTSTANDING SERVICE TO DISABLED EMPLOYEES OR BY A DISABLED EMPLOYEE

[REDACTED] (ITSD)

[REDACTED] was selected as chief of the Platform Support Unit (PSU) in August 2012. In a short time, her contributions made significant and lasting positive impacts on the FBI's mission. She was responsible for the development, operations, and maintenance of the database for the new UFMS. Her expert leadership and can-do attitude significantly enabled UFMS to be delivered on time in support of critical FD and DoJ objectives. Her superior management skill enabled numerous databases throughout the FBI to be operated and maintained at a high level at all times. She and the PSU received numerous laudatory comments from customers, personnel, and outside organizations because of her outstanding leadership.

She also reorganized the PSU to be more aligned with the ITSD's mission and to provide services to her customers. The PSU, consisting of five service teams: Data Migration, Sentinel, Infrastructure Upgrades, System Administration, and Transition, provided outstanding support.

ITSD Captures Top IT Innovator Award for DAVE and CTS

DAVE

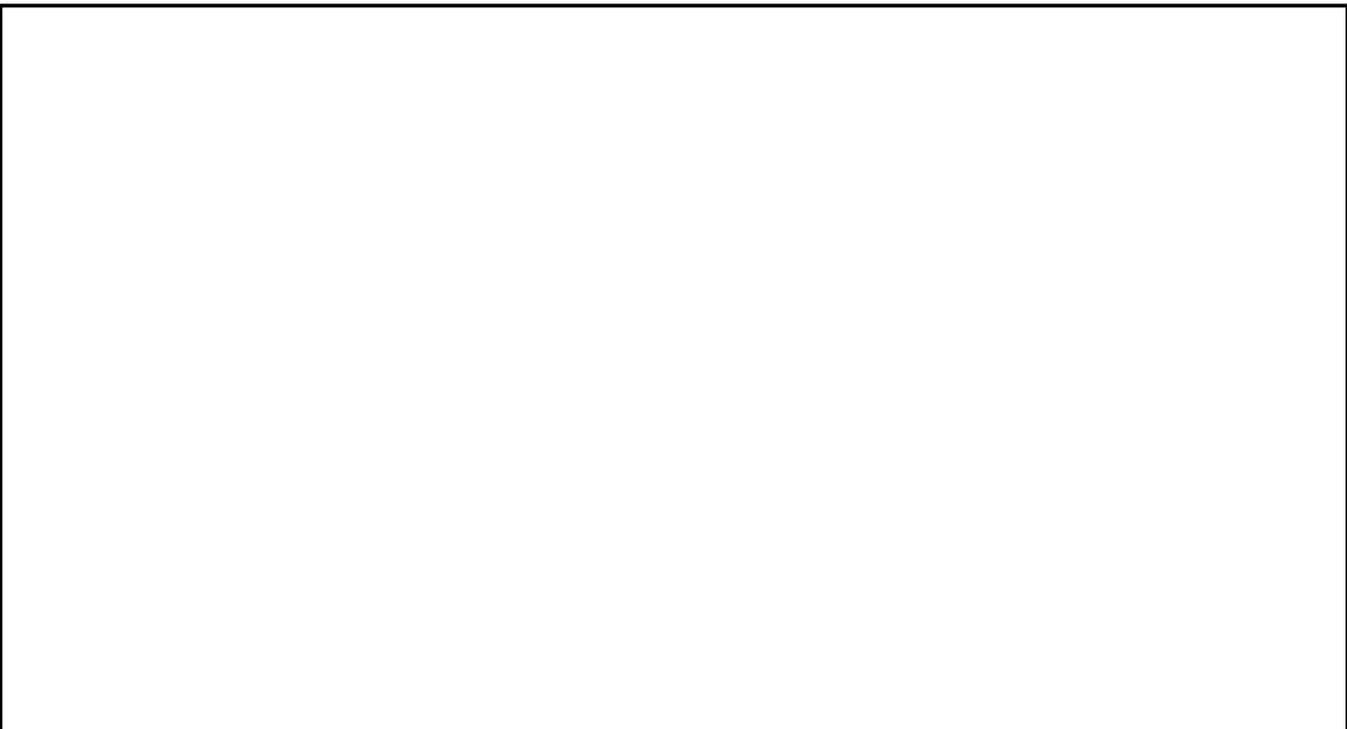
The ITB has become more creative in delivering innovative, cost-effective technology solutions to its workforce. Recently, two IT teams from the ITSD shared the top Government IT Innovator Award presented by InformationWeek magazine for their efforts in deploying a virtual server environment and data storage solution. This is the second time in three years that the FBI has captured this prestigious award.

In 2012, the Distributed Application Virtual Environment (DAVE) team developed a solution that consolidated more than 550 physical servers, virtualizing them so they fit into three racks of servers, enabling multiple operating systems, applications, and servers to run simultaneously. This consolidation effort allowed the ITSD to decommission and retire servers that were no longer needed, and saved the FBI \$800,000 in annual maintenance costs.

Virtualization allows the ITSD to be more flexible in deploying new services without the added cost of buying additional equipment and reclaims valuable staff time that can be used to provide better services to its customers.

In the DAVE environment, staff can build and deploy a new server in a matter of days instead of weeks, saving approximately \$2,000 per deployment in administrative

b6
b7C



b6
b7C

DAVE and CTS team

costs and in recovered work hours. DAVE is now supporting more than 1,500 virtual servers with more than 100 distributed applications and systems being used daily by FBI personnel worldwide. As DAVE matures, more applications are being developed and hosted in this virtual platform.

Another side benefit of DAVE is that it is helping the FBI become a "greener" workplace by enhancing efficiency and sustainability. Virtualization saves energy by eliminating power requirements previously needed to run all of the server equipment. With DAVE in place, the ITSD reduced its physical footprint at the FBIHQ data center from 20,000 square feet to 7,400 square feet at a new location. Fewer servers means lower cooling needs and maintenance, which translates into a huge energy cost savings of about \$450,000 for the FBI annually.

CTS

The CTS team's data storage and management solution was also recognized by InformationWeek magazine. The CTS team deployed a solution that uses a COTS product attached to the network, solely dedicated to providing file storage services for the FOs and RAs. This eliminated the need for the 188 file servers providing local shared disk access that required information to be saved to backup tapes which are expensive and time-consuming.

The CTS platform is proving to be a huge cost savings to the FBI in terms of resources. Using backup tapes was very time consuming and expensive. Savings are being realized as the field ITS staff no longer has to travel to retrieve the tapes. Now, they have the time to focus on other IT concerns at their office.

With the new CTS platform in place, the FBI now has five times more network storage to manage its information, which can be easily accessed via standard network protocols and tools.

Both the DAVE and the CTS platform are replicated in terms of operating systems, applications, and data at multiple sites. This ensures consistency between redundant resources and improves reliability and accessibility enabling COOP in the event of an emergency or disaster.



Innovative solutions such as DAVE and CTS are allowing the ITB to standardize IT hardware, simplify IT processes, and manage complicated operations and maintenance procedures at disparate locations. Both projects are proof that doing more with less can be very beneficial.



2013 Computerworld Honors Program

On June 3, 2013, AD Jeffrey C. Johnson, ITMD, accepted a Computerworld Honors Program Laureate Medal on behalf of the ITB Sentinel Agile Team.

The Honors Program recognizes those organizations that create and use IT to promote and advance the public welfare, benefit society and business, and change the world for the better.

Laureates were identified in 11 categories. The Sentinel Agile Team was recognized for its efforts to develop IT to measurably improve the safety and security of the user population. Laureates in this category are honored for their vision and determination with a spotlight on their exceptional work and tireless efforts to tap into the best of what technology can offer.

The Sentinel Agile Team received the medal for extending extraordinary efforts over a 22-month period to use innovation at every facet, as well as focusing on the FBI agents and analysts in developing the Sentinel Case Management System.

Knowledge Awards Program (KAP)

The FBI's KAP is a Bureau-wide awards and knowledge-sharing initiative that provides a way for employees to share proven solutions and best practices, knowledge, and experiences with the aim of helping the Bureau "do more with less" and foster the innovative spirit of the FBI workforce.

The FBI's Knowledge Office sponsored these awards. All approved submissions received a certificate and recognition at the Third Annual Knowledge Week event held May 1, 2013.

Submissions could include solutions that:

- Established methods to create, capture, or share knowledge
- Developed ways to promote collaboration and teamwork
- Promoted innovation and originality in the workplace
- Implemented successful business or process improvements

b7E

- Replicated best practices and lessons learned across the Bureau
- Improved or enhanced IT systems

The FBI Knowledge Office received 350 submissions; 234 met the requirements for qualification. Approximately 73 percent of the FOs and a majority of HQ divisions and offices participated. Twelve of the 234 solutions were selected as the best, based on the contribution that the solution made to the FBI mission. The ITB had 19 participants with 16 qualifying as meeting the requirements.

Employee Awards and Recognitions

During FY 2013, ITB employees received:

- 11 On-the-Spot Awards
- 14 Time-Off Awards
- 16 Lapel Pins

Employees were recognized for their individual performance, service, leadership, and teamwork. The funding for the FBI awards program was discontinued due to government budget cutting efforts.

2012 ODNI Science and Technology Award Winners

On Jan. 23, 2013, [redacted] (Computer Engineering Unit, STAS, ITED), cross-division Bureau team members, received the Office of the Director of National

Intelligence (ODNI) Science and Technology Award for their work developing and deploying the Binary Analysis, Characterization, and Storage System in support of the OTD's Investigative Analysis Unit. ●

ITB All-Hands Meetings

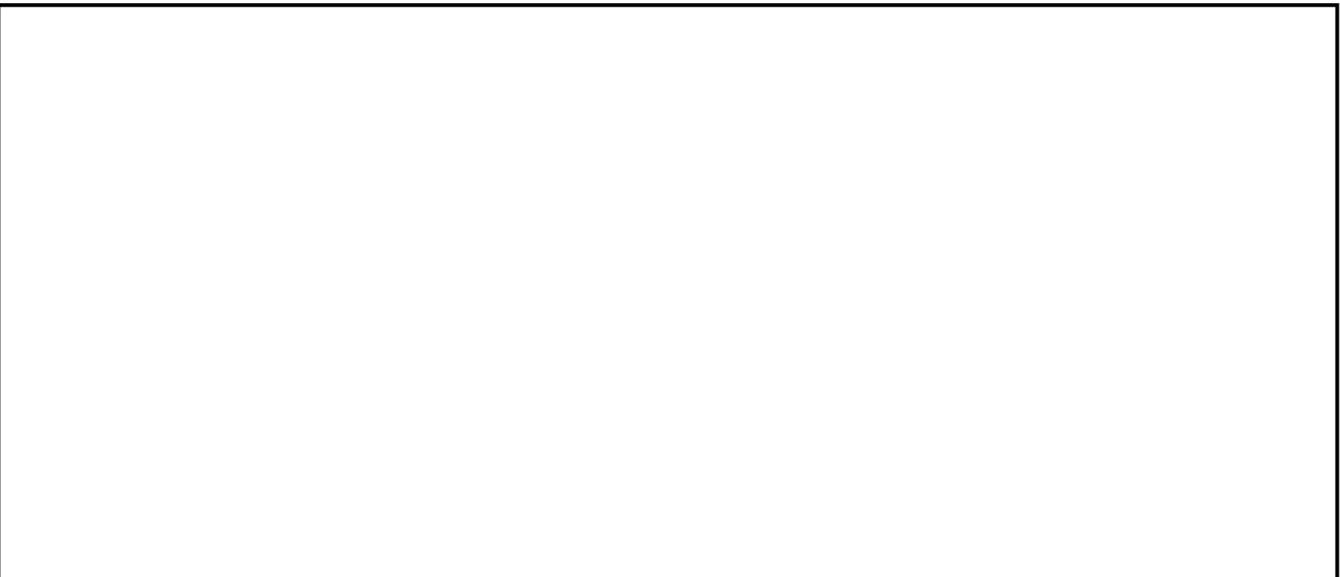
HIGHLIGHTS FROM THE MARCH 28 ITB ALL-HANDS MEETING

ITB employees were treated to a surprise visit from FBI Director Robert Mueller as they packed the Bonaparte Auditorium on Thursday, March 28, 2013, to hear from the EAD/CIO and ITB executives on recent branch initiatives. Director Mueller spoke on his commitment to ensuring that IT receives proper funding and resources, and named Windows 7® and the smartphone refresh as his top two ITB funding priorities. He also congratulated the ITB on the success of recent ITB projects, such as Sentinel [redacted] expressing his desire for the FBI to not fall behind in technology and to remain on the cutting edge.

The EAD/CIO addressed ITB guiding principles, such as meeting disaster recovery goals and developing and implementing thorough and transparent financial management processes. He reemphasized the ITB's three principles of teamwork: integrity, teamwork, and intelligent risk taking; and the four ITB business priorities: ensuring the trains run on time; IT business alignment; winning back the business; and financial responsibility. Among the ITB's numerous accomplishments over the past six months highlighted by the EAD/CIO, were the Exchange 2010 upgrade and network core upgrade to 10GB per second.

b7E

b6
b7C



2012 ODNI Science and Technology Award winners



b6
b7C

Director Mueller addresses ITB employees at All-Hands Meeting



b6
b7C

ITB executives answer audience questions at ITB All-Hands Meeting. From L-R: Deputy CIO Dean E. Hall, AD Jennifer R. Sanchez, AD Jeffrey C. Johnson, AD Carlo L. Lucchesi, and EAD/CIO Jerome M. Pender

The ITB executives briefed on initiatives they want to implement to improve Branch operations: data center strategy committee recommendations; ITB Requirements and Resource Allocation Board findings and recommendations; and service strategy improvements.

HIGHLIGHTS FROM THE SEPT. 16 ITB ALL-HANDS MEETING

ITB employees gathered on Sept. 16, 2013, in the Bonaparte Auditorium and via webcast to learn about recent Branch initiatives and accomplishments and to hear from executives about what has been occurring in their respective divisions.

EAD/CIO Pender spoke on the ITB's accomplishments over the past six months, such as the Windows 7 transition, NGSCION, the Windows 7 deployment, Provisioning Access Control, the Supervisory ITS (SITS) Rotational Program, and Centralized Tiered Storage.

EAD/CIO Pender spoke on his communications with Special Agents in Charge to better understand ITS concerns, such as disproportionate multi-function printer allocation regarding task force officers; broken and out-of-warranty laptop equipment; difficulties with Secure Video Teleconferencing communication; and issues with nonattributable browsing on the UNet.

SACs have had the opportunity to discuss other pressing issues, including budget constraints, the Sentinel integration with [REDACTED] SITS career ladders, and Electronics Technician/ITS network responsibilities.

AD Lucchesi, AD Johnson, and AD Sanchez briefed employees on important initiatives their divisions are implementing to improve Branch operations in FY 2014.

ITMD's Shadow Week

From April 15 through April 19, 2013, the ITMD hosted Shadow Week, a week-long professional development opportunity. The event was voluntary and open to all ITMD government employees.

ITMD participants shadowed unit chiefs, senior leaders, and executives, working one-on-one to experience first-hand the daily routine and responsibilities of the mentors. Pairing selections were based on matching the skills and knowledge of employees who wanted to shadow with the skills and knowledge of those volunteering to be shadowed.

Eight shadows and 12 mentors participated in the event. The shadows attended scheduled meetings and briefings with managers and received an overview of the ITMD's daily operations.



Virtual IT Exchange Seminar (VITES)

The VITES was held on Sept. 10 - 12, 2013. The theme of the seminar was "Focus on IT Engineering - Building Toward the future of Quality IT Services."

Each day, more than 250 employees from across the FBI's FOs, RAs, and HQ Divisions listened and participated in online presentations about a mixture of IT engineering and services. It was an opportunity for field IT staff to learn about new IT engineering initiatives and a forum for the ITB leadership to respond to questions and hear concerns raised by the field IT staff.

This is the second year that the ITSD held a virtual training workshop, primarily due to budget constraints; however, this was the first time that the event featured presentations from an IT engineering perspective. This was of particular interest because most of the field IT staff is involved in the deployment of hardware and software, but not with the development that goes into a project. Each presentation was followed by a short question-and-answer session where participants were able to ask the subject matter experts (SMEs) specific questions about the topic.

Cyber Table-top Exercise

More than 30 IT subject matter experts (SMEs) from the ITB, the OGC, the Office of Public Affairs (OPA), and the SecD participated in a table-top exercise at the ITB's Crystal City location on July 17, 2013.

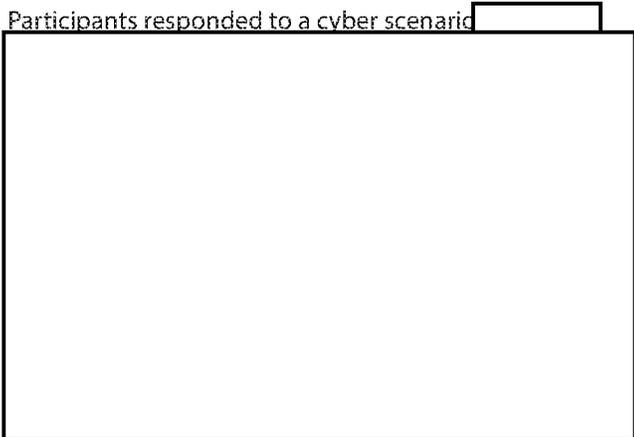
The half-day exercise, conducted at the request of Director Mueller and organized by the ITB with generous assistance from the Critical Incident Response Group, was designed to determine how the SMEs would collaborate, respond to an intrusion, and take the actions necessary to analyze, identify, and restore IT operations. This represented the first time these organizations formally participated in a collaborative exercise.

b7E

b6
b7C



Participants respond to a cyber scenario at Cyber Table-top Exercise



bring a wealth of knowledge from their government and private industry experiences.

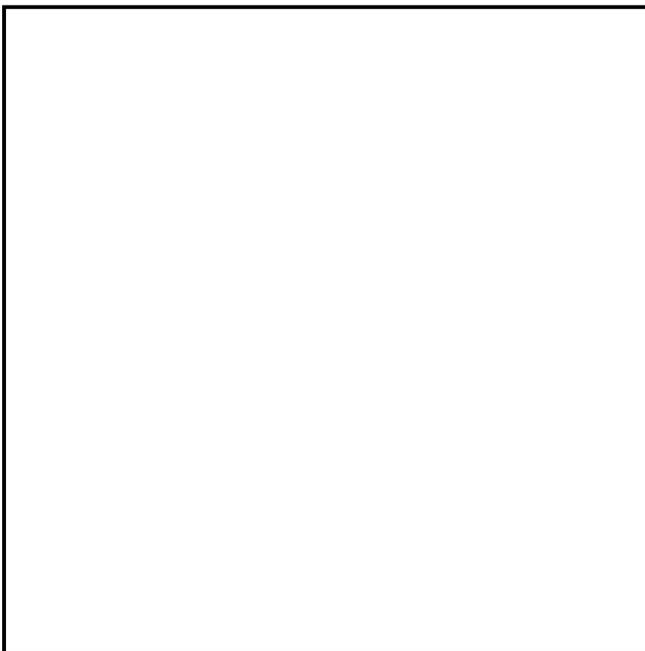
b7E

The ATG draws on the technical expertise and problem-solving skills of working group members to help the ITMD keep up with IT innovation. The ATG provides a platform for members to share ideas, enhance skills, and work to improve the division's business processes using technology. It is also aligned to the ITMD's SMS objectives.

As the groups reported out, it was clear that the exercise had provided a worthwhile opportunity for those who would actually be called on during such an event to meet, share their expertise, and build partnerships. The ITB leadership plans to host other exercises based on a variety of scenarios to ensure those responsible for protecting the FBI's IT operations and systems are well prepared for cyber combat.

Advanced Technology Group (ATG): Leveraging Technical Expertise

Since being formed in 2010, the ITMD's ATG has evolved into a group focused on leveraging the technical savvy and process-improving ideas of ITMD employees who



Members of ITMD's Advanced Technology Group

b6
b7C

The ATG is divided into “tiger teams” that act as an internal advisory group to identify and address internal gaps within the ITMD, ITB, or FBI, such as improving the ability to find information and share solutions division-wide and clarifying the promotion process and unclear development paths.

Still a relatively new working group, the ATG continues to use lessons learned to improve operations within the working group to make it more productive and a rewarding experience for its members. ATG leaders have learned that it is important to:

- Ensure members balance their collateral duties by managing their workloads with the voluntary responsibilities of the ATG;
- Understand and manage their expectations of working group members;
- Establish an internal organizational structure: chair, co-chairs, tiger team points of contact, and working group members to prioritize and distribute tasks;
- Restructure tiger teams, if necessary, to avoid interrupting workflow and to provide flexibility to working group members.

The ATG’s members meet every month for tiger team project discussions, and every six months for brainstorming sessions. ATG chairs also brief the ITMD’s DAD every quarter. Membership in the ATG is open to all ITMD employees.

Damascus Students Participate in IT Job Shadow Day

The Federal CIO Council hosts an IT Job Shadow Day for high school students to attract talented students to possible internships or future careers with the U.S. Government. Students spend a day learning about the latest technologies and processes used by federal employees to automate services, provide critical data, and secure information.

The IT Job Shadow Day attracts more than 2,000 students a year from around the country to see how the government IT workforce supports the daily operations of DoJ component agencies. This affords a great opportunity for rising high school juniors and seniors to learn about the FBI’s mission.

On May 1, 2013, the ITB and the OPA jointly hosted the Academy of IT club from Damascus High School in Montgomery County, Md. The group of 20 students participated in the IT Job Shadow Day by touring both the DoJ Security Operations Center and the FBI Strategic Information and Operations Center (SIOC). While in the SIOC, students learned the advanced technologies the FBI employs to accomplish its mission needs, such as the tracking devices provided to Legat employees for personnel recovery and collection during emergency situations.

ITED AD Carlo Lucchesi and EAD/CIO Jerome Pender spoke with the students about the technology



Academy of IT Club from Damascus High School participate in IT Job Shadow Day

b6
b7C

opportunities and challenges facing the FBI IT workforce. During his presentation about the ITB, AD Lucchesi told the students about various ITB projects, such as the Case Management System and e-Portfolio, and described the vast information flow among the 56 FOs, 400 RAs, and international Legats.

He explained, "We're the ones in the background making sure the information gets to the right place at the right time." After all the students raised their hands when asked if they came into the building with a mobile device, EAD/CIO Pender then discussed the challenges the FBI faces as the agency moves to a more mobile computing platform. The group ended their day with a quick tour of the updated FBI Educational Tour, including the chance to see a few FBI agents qualifying on the indoor gun range. The students left the FBI headquarters with a more in-depth view of the ITB and gift bags slung across their backs reading: "Wanted by the FBI: Working for a safer tomorrow."

he visited each vendor to give allotted time for them to share their products with him.

- On April 16, 2013, ITED hosted an IT Security Vendor Day, in an effort to keep FBI employees informed of new IT security products, technologies, and services available in the industry. Over 50 small businesses and prime

TECH DAY @ FBIHQ

Wednesday, August 14, 2013
William Webster Conference
Room (Flag Room)
FBIHQ Room 1236
10:00 a.m. - 2:00 p.m.

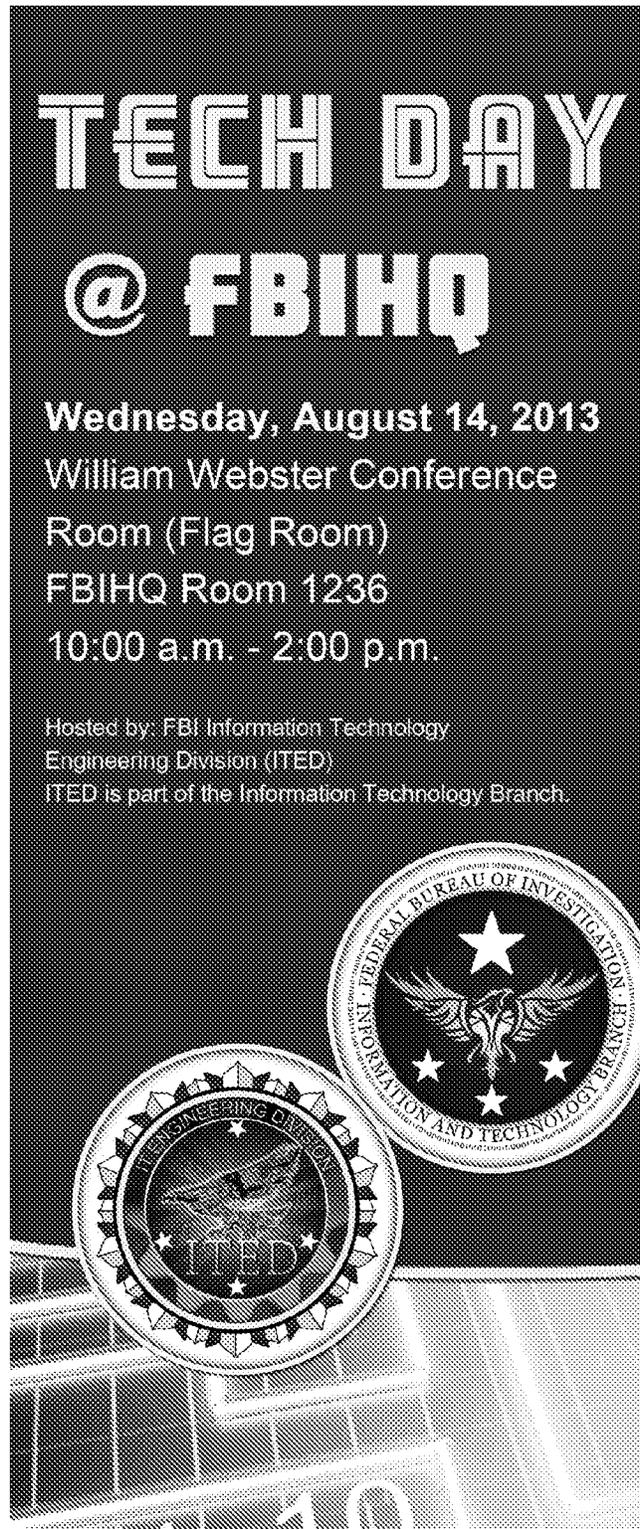
Hosted by: FBI Information Technology
Engineering Division (ITED)
ITED is part of the Information Technology Branch.

Vendor Day events

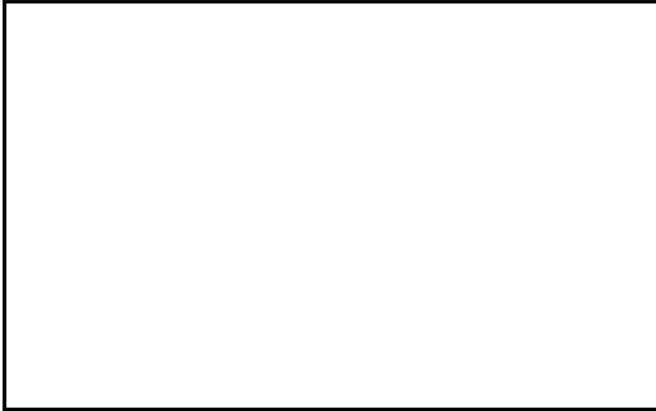
Vendor Days

During FY 2013, the ITED hosted four Vendor Day events. These gatherings, held in the William H. Webster Room at FBIHQ, provided professional venues for educating attendees and keeping them current on new IT products and industry trends.

- On Oct. 16, 2012, the ITED hosted the Mobility Computing Expo. Many FBI personnel took the time to walk around and speak with the various vendors who were represented at this event.
- On Feb. 19, 2013, the ITED hosted the first Vendor Day of the calendar year. The theme was a general theme of: FBI IT Vendor Expo. Over 50 vendors participated in this event with hopes of sharing their products with potential FBI employees. EAD/CIO Jerome Pender addressed the vendors and participating audience, giving an overview of the ITB and its expectations. EAD/CIO Pender also introduced his executive staff to the audience. After his presentation



b6
b7c

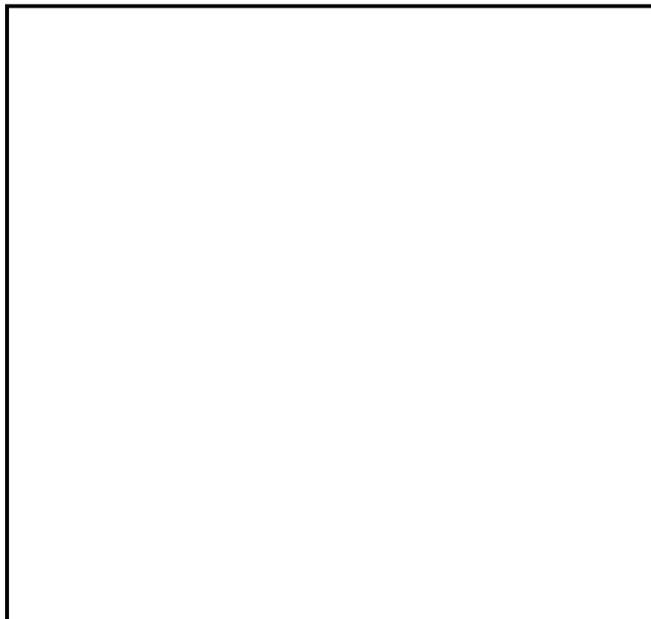


Vendor Day events

contractors with the latest technologies were on-site to share information about their companies and how their IT security solutions may be utilized by the FBI. AD Jennifer Sanchez addressed the vendors and participating audience to give insight on the FBI's priorities pertaining to the ITB.

- On Aug. 14, 2013, ITED hosted a Tech Day at FBIHQ. More than 50 small businesses and prime contractors participated. This event focused on the Sequestration of the FBI. Participating vendors were given the opportunity to present their products in the mindset of the Sequestration that is facing the FBI. AD Carlo Lucchessi addressed the vendors and participating audience giving knowledge of the upcoming budget cuts the FBI would be facing.

The ITED coordinates these events and plans to continue hosting these highly successful events in the future.



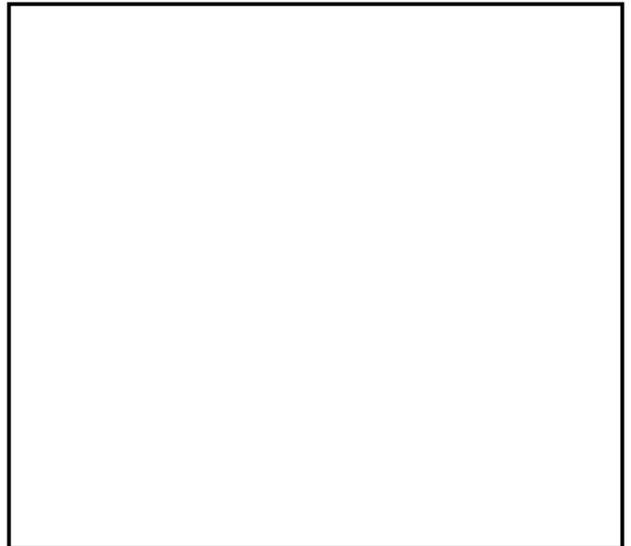
AD Hope receives CFC Award for ITMD's fund-raising efforts

Combined Federal Campaign (CFC)

b6
b7c

The FBIHQ CFC took place Oct. 17 – Dec. 15, 2012. The voluntary campaign provides an annual opportunity to help others in need by donating to local, national, and international human, health, and environmental service organizations. Volunteer coordinators and key workers are instrumental to running a successful campaign.

A variety of fundraising events raised additional monies for the CFC program. Some of the ITB's fundraising activities included bake sales, a morning coffee-cart, a chili cook-off, and a fish fry event.



Chili Cook-off

The ITED collected a total of \$17,178.78. ITED participants included one Eagle (marking an individual donating one percent of his/her annual salary) and one Double Eagle (marking an employee donating two percent of his/her annual salary).

The ITMD raised a total of \$20,225.55.

The ITSD raised a total of \$33,790.06.



Morning Coffee-cart

b6
b7C



Fish Fry Event

Even amid financial uncertainty, the fundraising campaign was a resounding success. The ITB's employees made a difference to an untold number of lives.

ITMD Shines in the National Police Week 5K Race

On Saturday, May 11, 2013, for the third year in a row, team 324 RUN! ran in the National Police Week 5K. This year, team 324 RUN! placed 4th overall out of a total 71 teams and was comprised of several employees from across the FBI, as well as their family members.

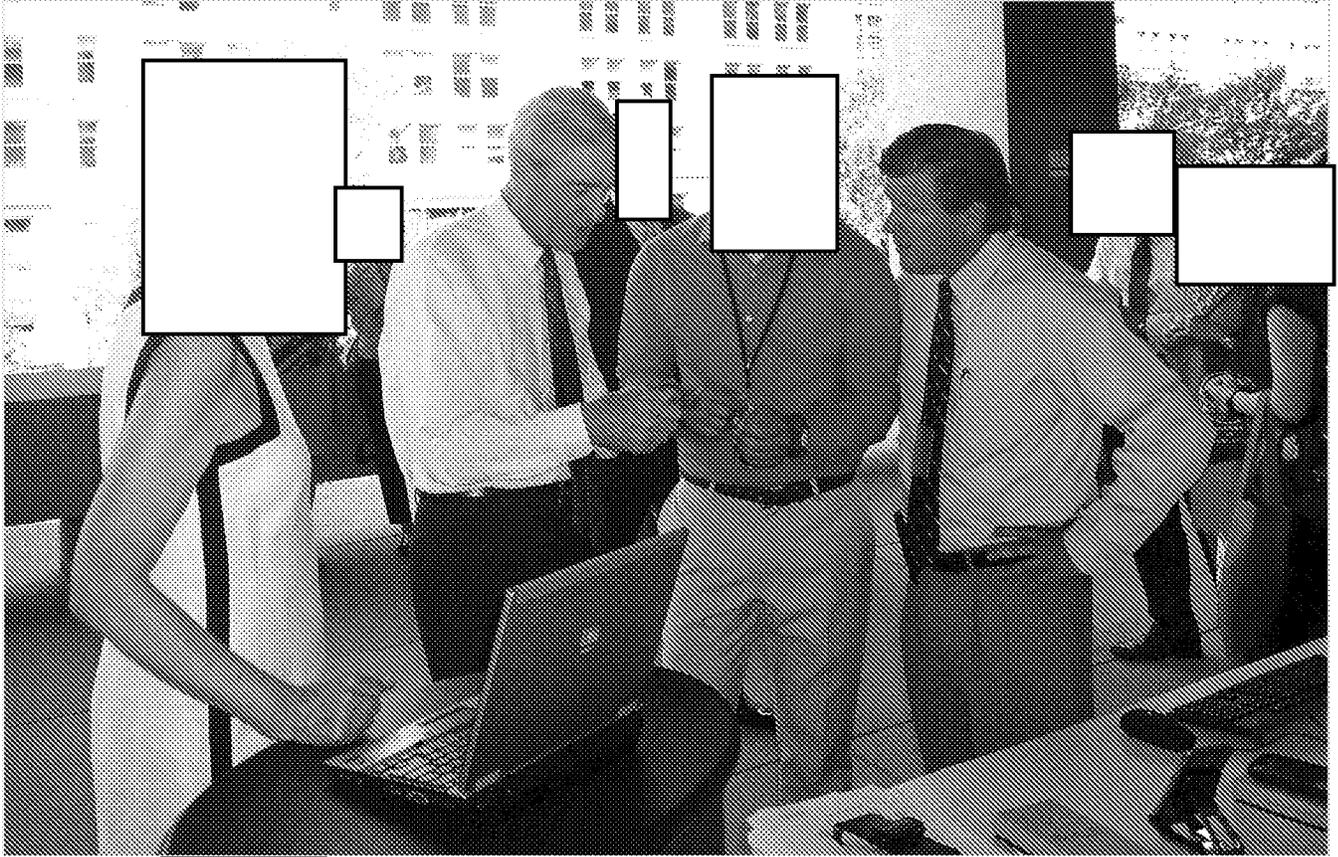
The National Police Week 5K is hosted by the Officer Down Memorial Page (ODMP) to honor fallen law enforcement officers by raising awareness of the sacrifices officers make every day. The event raises money to support ODMP programs and Concerns of Police Survivors to support important programs that assist survivors after the loss of a loved one.



ITMD Christmas Party



Team 324 RUN!



b6
b7C

Computer Scientist [redacted] ITED, demonstrates the FBI's new smartphone to Director and Mrs. Mueller and AD Michael P. Kortan, OPA

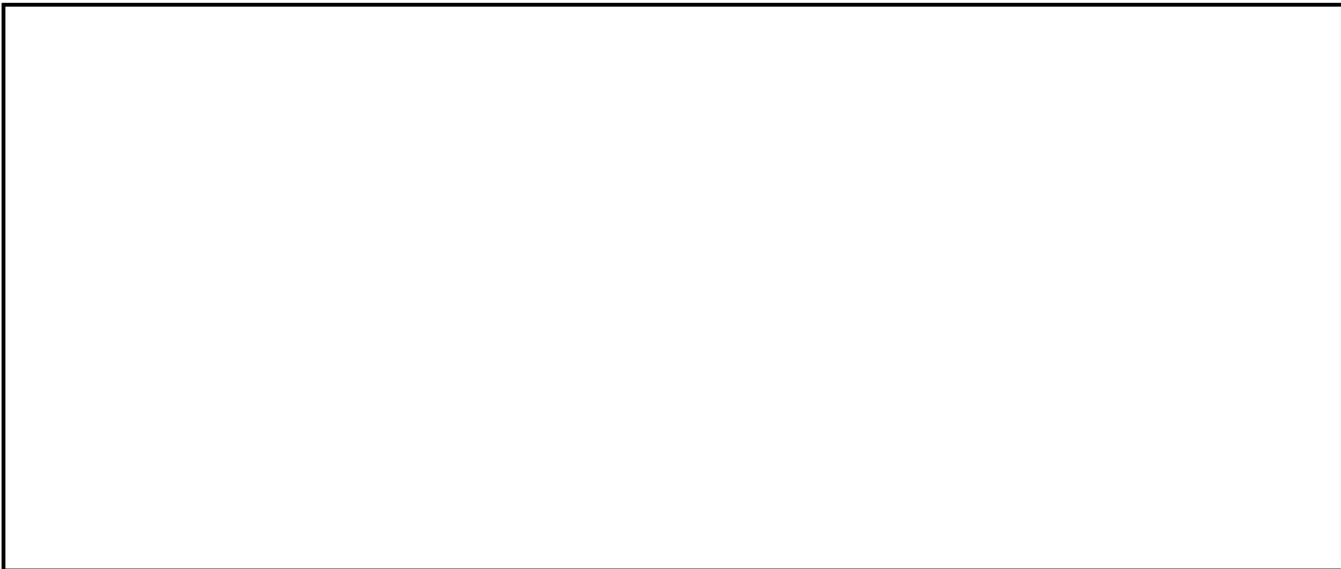
Family Day

The ITB participated in the annual FBI Family Day held on June 28, 2013, at FBIHQ. The ITB manned a multi-project booth on the mezzanine level and a table with a variety of children's activities in the William H. Webster Conference Room.

Demonstrations included the unveiling of the new FBI smartphone that will replace the BlackBerry device,

Windows 7, and FANTOM's Network Analysis capabilities. The FANTOM demonstration included a fun dataset for the children that showed them the relationship between heroes and villains in the Marvel universe. An additional display highlighted photos of ITB events held during FY 2013.

The ITB took advantage of the event to conduct videographic interviews of customers and used those interviews for the Voice Over IT employee newsletter. ●



b6
b7C

ACS	Automated Case Support
AD	Assistant Director
ADD	Associate Deputy Director
AMP	Advanced Management Program
ATG	Advanced Technology Group
BIKR	Bureau IT Knowledge Repository
CFC	Combined Federal Campaign
CHS	Confidential Human Source
CIO	Chief Information Officer
CIRG	Critical Incident Response Group
CJIS	Criminal Justice Information Services
CMT	Classification Marking Tool
COOP	Continuity of Operations
COTS	Commercial-off-the-Shelf
CPS	Clearance Processing System
CTD	Counterterrorism Division
DAD	Deputy Assistant Director
DAVE	Distributed Application Virtual Environment
DI	Directorate of Intelligence
DO	Director's Office
DOJ	Department of Justice
EAD	Executive Assistant Director
ECC	Enterprise Circuit Consolidation
EOC	Enterprise Operations Center
EPAS	Enterprise Process Automation System
ERAS	Enterprise Remote Access Service
ESS	Executive Staff Section
FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FBINet	FBI Classified Network
FD	Finance Division
FLSD	Facilities and Logistics Services Division
FO	Field Office
FY	Fiscal Year
HRD	Human Resources Division
IC	Intelligence Community
IT	Information Technology
ITAMP	IT Asset Management Program
ITB	Information and Technology Branch
ITED	Information Technology Engineering Division
ITMD	Information Technology Management Division

b7E

ITS	Information Technology Specialist
ITSD	Information Technology Services Division
KAP	Knowledge Awards Program
LCM	Life Cycle Management
LEO	Law Enforcement Online
Legat	Legal Attaché
MFP	Multi-Function Printer
NGIC	National Gang Intelligence Center
NGSCION	Next Generation Sensitive Compartmented Information Operational Network
NNCP	National Name Check Program



b7E

OCKO	Office of the Chief Knowledge Officer
OGC	Office of the General Counsel
OMB	Office of Management and Budget
OTD	Operational Technology Division
PAC	Provisioning and Access Control System
PHA	Project Health Assessments
RA	Resident Agency
RITS	Regional Information Technology Specialist
RMD	Records Management Division

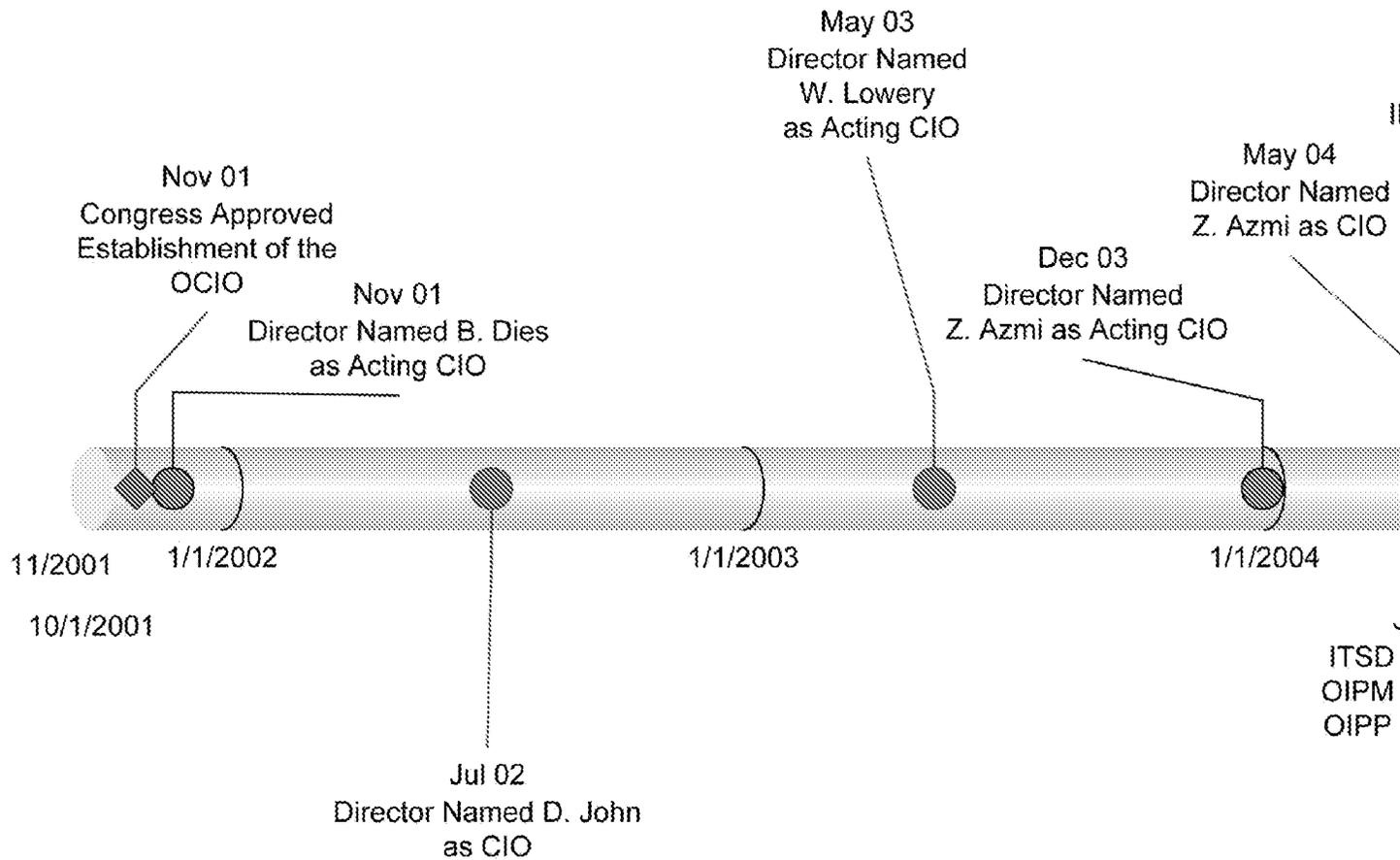


SCI	Sensitive Compartmented Information
SCION	Sensitive Compartmented Information Operational Network
SecD	Security Division
SMS	Strategy Management System



SPL	Standard Products List
STAS	Special Technologies and Applications Section
TS	Top Secret
UFMS	Unified Financial Management System
UNet	FBI Unclassified Network
VITES	Virtual Information Technology Exchange Seminar

History of Office of the Chief Information Officer FY2001-

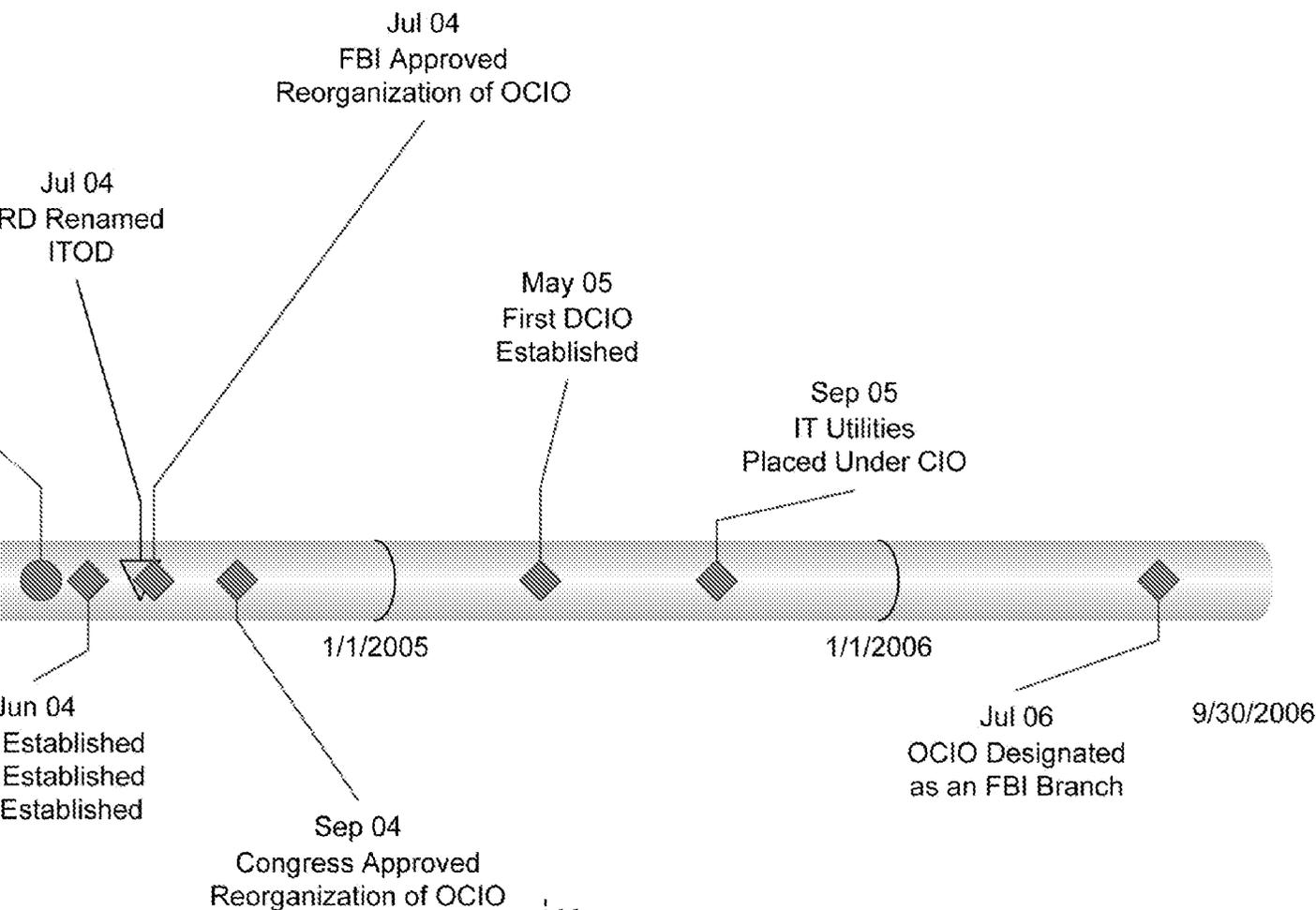


ITSD
OIPM
OIPP

Legend

- Personnel Changes
- ▽ Component Name Changes
- ◇ Component/Position Established

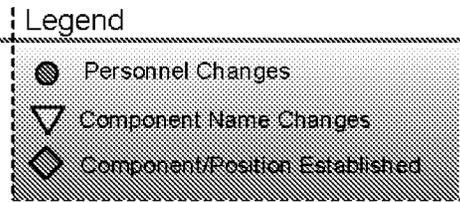
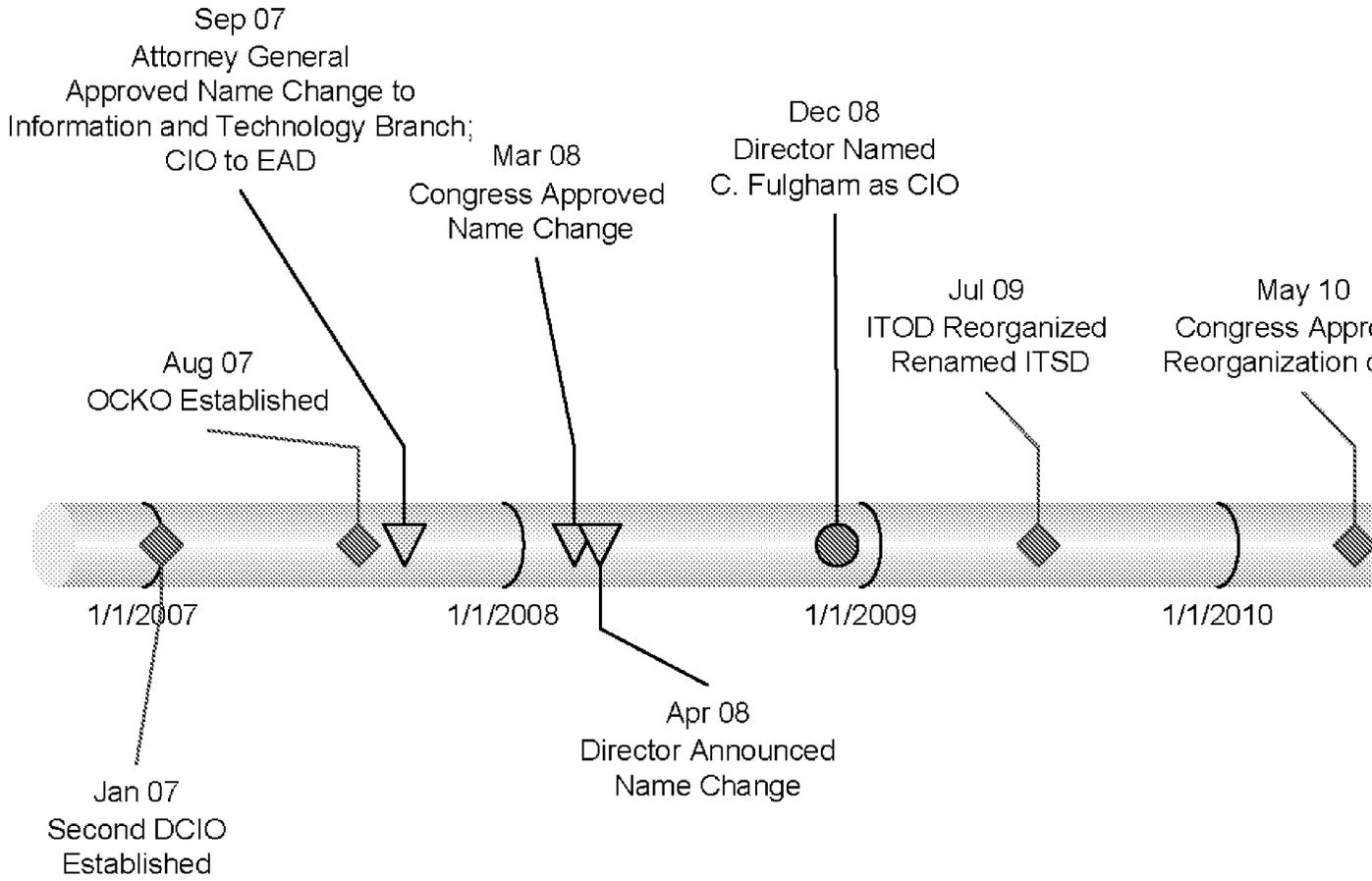
Officer/Information and Technology Branch
- FY2006



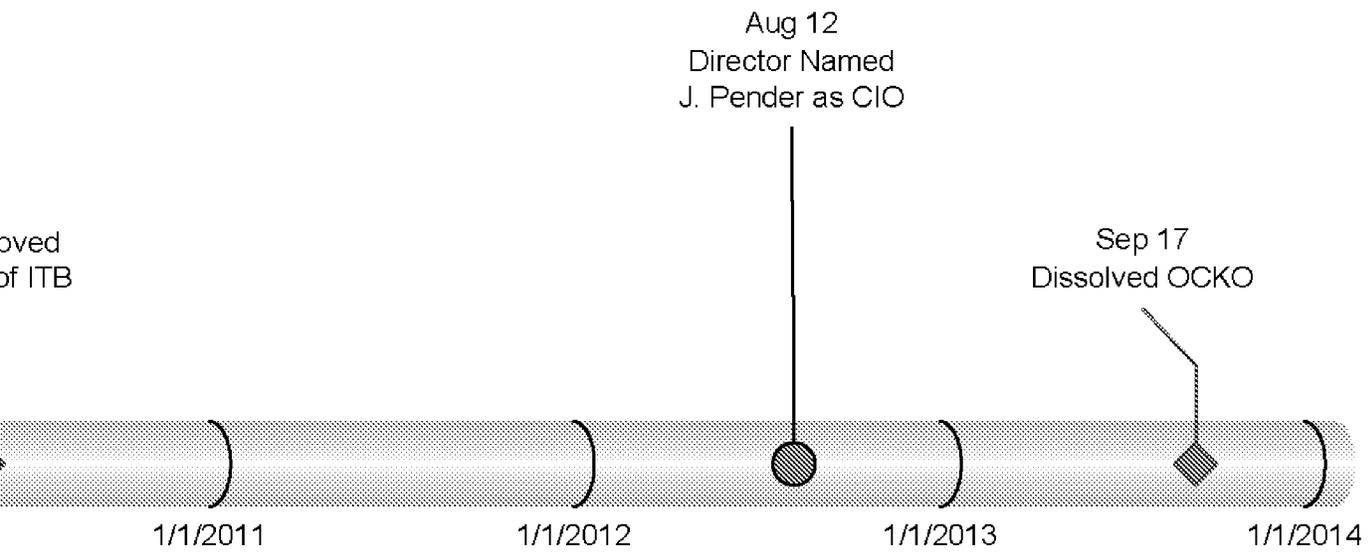
Key

CIO	Chief Information Officer
DCIO	Deputy Chief Information Officer
IRD	Information Resources Division
ITOD	IT Operations Division
ITSD	Office of IT Systems Development
OCIO	Office of the Chief Information Officer
OIPM	Office of IT Program Management
OIPP	Office of IT Policy and Planning

History of Office of the Chief Information Officer FY2007



Chief Information Officer/Information and Technology Branch - FY2012



Key

- CIO Chief Information Officer
- DCIO Deputy Chief Information Officer
- EAD Executive Assistant Director
- ITB Information and Technology Branch
- ITOD IT Operations Division
- ITSD IT Services Division
- OCKO Office of the Chief Knowledge Officer

ACKNOWLEDGEMENTS

This publication was produced by the
ITB Executive Staff Section, Communications and Outreach Unit.

Thanks to all ITB staff who collaborated and contributed to this effort.

The report may be viewed online at FBI Ne

b7E



OFFICIAL FBI PUBLICATION

U.S. Department of Justice
Federal Bureau of Investigation
Information and Technology Branch