U.S. Department of Justice
Federal Bureau of Investigation

FBI Information Sharing & Safeguarding Report 2012

Mission
Programs
Infrastructure
Policy

FBI Information Sharing and Safeguarding Report 2012

"The most effective weapon against crime is cooperation…
The efforts of all law enforcement agencies with the
support and understanding of the American people."
J. Edgar Hoover

This quote from J. Edgar Hoover is prominently displayed on a courtyard wall of the FBI Headquarters in Washington DC. The FBI has for many years recognized the value and the necessity of cooperation between law enforcement and the American people, and among the agencies that serve them. The foundation of this cooperation is mutual respect, trust and the sharing of information both within the government, and between the government and its citizens. As the FBI Chief Information Sharing Officer, my zeal for information sharing rests firmly on this foundation. It is the right of all Americans to be sure that their government is not only providing security to the nation as a whole, but also to each of us individually by guarding our civil rights and civil liberties.

The goal of the FBI regarding the sharing of information is to prevent the activities of those who would do us harm through acts of terrorism or other crimes. Information sharing naturally facilitates this basic FBI mission. Furthermore, the idea that we should have transparency in government underpins the very purpose for information sharing. We absolutely have to be balanced - we must protect some information in our care to safeguard citizens' privacy and civil liberties, as well as to shield our sources and methods. Our investigative agencies must wait until the activities of the persons under investigation reach a level of validity and clarity before the information is shared. With this sense of steadiness in our approach, we can have the transparency of government that allows our citizens to have greater visibility into the workings of government, reduce crimes and terrorism, and help to produce a greater wealth of knowledge and societal progress.

Reaching for transparency and balancing the responsibility to share with the need to safeguard will result in crime prevention. At the same time, this balance will protect the constitutional rights of citizens, adding the value to our society that the FBI can be proud of.

C. Elaine Cummins, PhD
Chief Information Sharing Officer
FBI

I. Executive Summary

The sharing and safeguarding of critical information fundamentally enable the unique national security and law enforcement missions of the Federal Bureau of Investigation (FBI). Continued and significant progress in sharing and safeguarding characterized the FBI in 2012. With significant enhancements to several of its technical and operational sharing and safeguarding capabilities in 2012, the FBI reaffirmed its commitment to responsibly sharing timely, relevant, and actionable intelligence with the widest appropriate audience while protecting the privacy and civil liberties of the American people.

In 2012 the President signed the National Strategy for Information Sharing and Safeguarding (NSISS), setting the stage for implementation of significant new initiatives and the continued structural, technical, and cultural advancements across the U.S. Government to further enhance national security. The FBI provided significant input to the strategy, and participated throughout 2012 in the coordination of the strategy's implementation guidance soon to be published.

The FBI continued to lead and participate in significant information sharing initiatives in 2012. This report, presented by the FBI Chief Information Sharing Officer (CISO), provides a summary of the many activities ongoing throughout the past year. The report is presented again this year in a format intended to mirror strategic issues and initiatives across the entire U.S. Government's diverse information sharing environment.

The FBI made several organizational changes in 2012, in part to enhance the visibility and effectiveness of information sharing and safeguarding. These changes included a realignment of Knowledge Management and Information Sharing executives to give them greater ability to shape and guide enterprise-wide information access and sharing policy; and reorganization of the FBI's Directorate of Intelligence (DI), which will enhance partner engagement and information reporting. In addition, the FBI undertook in 2012 a revision of its data access policies and implementation to better align with U.S. Government initiatives toward Attribute Based Access Controls for data.

In 2012 strategic integration of technology and the continued evolution of sharing and safeguarding cultural changes increased FBI capacity to discover, access, share, and exploit information. Developments in technology tools and databases enhanced internal sharing and safeguarding of mission support, while organizational and cultural changes within the FBI itself significantly improved sharing with external partners throughout the year. Of particular note, in 2012 the FBI's Law Enforcement National Data Exchange (N-DEx) system made new categories and unprecedented amounts of information more accessible to the entire Justice Community.

The FBI reaffirms its commitment to effectively and efficiently share information responsibly with authorized partners for mission success; and to safeguard sensitive information to protect privacy, civil liberties, and national security.

NOTE: The contents of this report are organized according to the U.S. Intelligence Community's goals and objectives for information sharing and safeguarding.

The following graphic "The Information Sharing Environment" visually summarizes the information sharing and safeguarding environment for the FBI.

II. Recent Highlights

The year 2012 was marked by significant change within the FBI regarding information sharing and safeguarding. In response to numerous challenges and potential threats, the FBI took steps to more effectively and efficiently share vast amounts of information with Law Enforcement and Intelligence Community partners, as well as to better protect sensitive information to preserve the integrity of operations while ensuring the privacy and civil liberties of U.S. persons. Several major developments are worth highlighting below.

- In 2012 the FBI began a reorganization of the Office of the Chief Knowledge Officer (OCKO) and the Chief Information Sharing Office to better align their respective functions, both to senior leadership and to one another. These changes are designed to ensure higher visibility of information sharing and safeguarding issues and should be completed in 2013.

- Also in 2012, the FBI streamlined the structure of the Directorate of Intelligence (DI) so it could more effectively provide strategic direction, program management, policy oversight, and support to the entire Intelligence Program. This realignment of structure and resources allowed the FBI to transfer certain functions—including domain management, collection management, targeting, tactical analysis, strategic analysis, and finished intelligence production—from the DI to the FBI's operational divisions at FBI Headquarters, enabling intelligence to more effectively drive the organization's operations.

- The FBI expanded information in the National Data Exchange (N-DEx) this past year to provide vast new amounts of data regarding ongoing investigations to authorized law enforcement partners while still respecting privacy and civil liberties. By the end of 2012, over 70,000 users have access to N-DEx, while approximately 4,000 agencies are submitting data, representing more than one billion entities (persons, places, things, and events). In 2012 N-DEx also expanded to include records and users from corrections, probation, parole, courts, and prosecuting attorney's offices.

- Finally, in 2012 the Bureau undertook a major effort to revise its data access control system for all data held within the FBI. Attribute-based access controls will greatly enhance internal sharing while more effectively protecting sensitive information, and at the same time facilitate responsible sharing of selected information with authorized partners external to the FBI.

III. Optimizing Information Sharing with Partners to Enable Decision Advantage

Few national security or law enforcement missions can be accomplished by the FBI working alone. The FBI understands the critical value of partnership, and remains committed to strengthening ties at all levels, from local to international. The FBI National Information Sharing Strategy (NISS) provides the common vision, goals, and framework needed to guide information sharing initiatives with Federal, State, local, and Tribal agency partners, foreign government counterparts, and private sector stakeholders. Through enhanced understanding of their diverse needs, the FBI is able not only to improve the collection, exchange, and protection of information, but also to leverage partner capabilities to mitigate and defeat threats to the United States, its citizens, and infrastructure. The FBI continues to improve its understanding of partners' needs, evolving its own organization to strengthen partnerships, continue major sharing initiatives, and leverage other capabilities to better share and safeguard information.

A. Understanding Needs

The FBI uses a variety of mechanisms to ensure that it understands the information sharing and safeguarding needs of its partners, as it also shares its own needs with them. These mechanisms range from day-to-day operational activities, to regular liaison and engagement, formal interaction with specified groups, and includes involvement of the FBI's Privacy and Civil Liberties Officer and the Privacy and Civil Liberties Unit (PCLU) in the Office of the General Counsel (OGC).

Operational coordination

The ongoing efforts of the FBI's Joint Terrorism Task Forces (JTTFs) and the JTTFs' embedded Terrorism Liaison Officers (TLOs), along with other operational task forces and joint operations, ensure that intelligence and information requirements are well understood, and in so doing effectively support national security and law enforcement operations.

Mutual understanding through engagement

The FBI maintains regular liaison and engagement through FBI Field Offices (FOs), Field Intelligence Groups (FIGs), Regional Intelligence Groups (RIGs), other liaison and attaché roles, and outreach programs such as the Domestic Security Alliance Council (DSAC), InfraGard, and the Department of State (DOS) Overseas Security Alliance Council (OSAC). Informal contact at international, national and regional conferences and symposia also improve understanding of information sharing requirements. In addition, the Interagency Threat Assessment and Coordination Group (ITACG) facilitates both mutual understanding of needs and direct sharing efforts among Federal, State, local, and Tribal authorities.

Interagency Threat Assessment and Coordination Group

The ITACG is a joint FBI/Department of Homeland Security (DHS)/National Counterterrorism Center (NCTC) initiative in which personnel research, integrate, analyze, draft, and assist in the dissemination of Federally coordinated information to State, local and Tribal, and private sector (SLTP) entities within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information. State, local, and Tribal law enforcement, fire and emergency medical services, and public health personnel assigned to the ITACG work with FBI,

DHS, and NCTC personnel to ensure first responder needs are understood by the national counterterrorism community and are represented in intelligence production.

On a daily basis, FBI personnel assigned to the ITACG capitalize on information sharing and effectively fulfill customers' needs by researching, drafting, editing, and briefing relevant intelligence which has potential relevance to the first responder community. In 2012 FBI assignees, along with other ITACG members, reviewed or edited 191 finished intelligence products from the first responder perspective, a 50% increase over 2011. During this same period, FBI ITACG assignees assisted in nominating 1,380 articles for inclusion in the NCTC daily *Terrorism Summary*, with over half of these submissions accepted. FBI ITACG assignees also facilitated over 30 requests for product classification downgrades to enable a broader readership at the SLTP-level. In addition to producing 12 ITACG-generated *Roll Call Release* products in 2012, FBI assignees played a significant role in developing and coordinating a new intelligence product line, *Fire Line*, specifically intended to meet the unique intelligence needs of over one million fire service members nationwide. Furthermore, on a bi-weekly basis, FBI ITACG assignees briefed current terrorism threats to over 20 state and local fusion centers via secure video teleconferences, creating an efficient synchronization of effort forum which enabled the exchange of intelligence inputs, concepts, and ideas. In 2013 the FBI will coordinate with DHS and other stakeholders regarding a new entity to continue the work of the ITACG.

B. Continuing to effect changes within the FBI itself

In 2012, the FBI completed a comprehensive review of its Intelligence Program and undertook significant organizational and procedural changes to improve the responsiveness of the DI. Also in 2012, the FBI streamlined the structure of the Directorate of Intelligence (DI) so it could more effectively provide strategic direction, program management, policy oversight, and support to the entire Intelligence Program, including the following key initiatives:

- Threat Review and Prioritization
- Domain, Collection, and HUMINT Program Management
- Domestic DNI Representative Program and Joint Regional Intelligence Groups
- Raw and Finished Intelligence Production Management
- Foreign Language Support
- Information Technology Interoperability
- Intelligence Program Policy and Workforce Strategy

This realignment of structure and resources allowed the FBI to transfer certain functions—including domain management, collection management, targeting, tactical analysis, strategic analysis, and finished intelligence production—from the DI to the FBI's operational divisions at FBI Headquarters, enabling intelligence to more effectively drive the organization's operations. Threat-based fusion cells within each investigative program now serve as intelligence teams to integrate all aspects of the intelligence cycle, providing a more strategic, flexible, and nimble approach to identifying and mitigating current and emerging threats. In addition, a standardized business process now guides the work of these fusion cells, allowing the FBI to identify and respond to threats more effectively and efficiently.

In late 2012 the FBI's executive leadership decided to raise the visibility of information sharing and safeguarding to address potential vulnerabilities and better leverage opportunities. In 2013 the Office of

the Chief Knowledge Officer (OCKO) will be reorganized to include the Chief Information Sharing Officer, and to place the new OCKO higher in the Bureau structure, reporting to the Associate Deputy Director. The Chief Knowledge Officer (CKO) will also chair the Information Sharing Policy Board (ISPB), which reviews and approves all significant information management and sharing policy matters. These changes are intended to raise the visibility of all information sharing and safeguarding issues, and ensure that these matters receive prompt and focused attention at the highest levels.

C. Continuing major sharing initiatives with partners

Major sharing initiatives with partners range from operational organizations such as the JTTFs, to broader nationwide initiatives including suspicious activity reporting, general law enforcement sharing through portals such as the Law Enforcement Online (LEO) system, and specifically designed systems for sharing of incident or case data such as N-DEx. In addition, broad engagement with State and local fusion centers and Tribal and border communities provide numerous opportunities to enhance sharing. Finally, there are specific initiatives in the areas of cyber crime, drugs, gangs, and other crimes.

National Joint Terrorism Task Force (NJTTF) and Joint Terrorism Task Forces (JTTFs)

The FBI-led National Joint Terrorism Task Force (NJTTF) is a multi-agency task force consisting of 42 government agencies and critical-industry representatives collocated at the National Counterterrorism Center (NCTC). The mission of the NJTTF is twofold: 1) to enhance communications, coordination, and cooperation concerning terrorism intelligence among Federal, State, local, and Tribal government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, and homeland security communities; and 2) to support the JTTFs throughout the United States.

Located in more than 100 cities across the United States — including one in each of the FBI's 56 field office locations — JTTFs comprise small teams of highly-trained, locally-based investigators, analysts, linguists, Special Weapons And Tactics (SWAT) experts, and other specialists from dozens of Federal, State, local, and Tribal law enforcement organizations and Federal intelligence agencies. JTTFs investigate leads, gather evidence, make arrests, provide security for special events, conduct training, collect and share intelligence, and respond to threats and incidents swiftly.

JTTF Success Story

The Alaska Information and Analysis Center (AKIAC), in coordination with the Alaska JTTF, issued an Officer Safety Bulletin on two potentially violent individuals believed to be illegally armed and departing from Canada. The AKIAC used liaison officers with the Royal Canadian Mounted Police and U.S. Customs and Border Protection (CBP) to ensure that the Canadian Border Security Agency (CBSA) received this information and was on alert. As a result, CBSA conducted a high-risk inspection at a port of entry, and discovered a weapon. The suspect was denied entry into Canada, turned around, and was then stopped at the CBP checkpoint, where he was arrested by Alaska State Troopers.

JTTF Success Story

The Lakewood, Colorado, Police Department received information that an individual had placed two improvised explosive devices at a Borders bookstore at the Colorado Mills Mall. Due to the nature of the crime, the Lakewood Police Department notified the FBI of the incident, who in turn activated the JTTF. Agents from the JTTF and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) responded to the scene and began collecting information, which they passed to the Colorado Information Analysis Center (CIAC). A few hours later, the CIAC sent information to fusion centers nationwide and Terrorism Liaison Officers (TLO) statewide, requesting any information potentially relating to the incident. Less than 15 minutes after sending this information to Colorado TLOs, the CIAC received vital information from a State Trooper. Approximately twenty-four hours earlier, the suspect had crashed his vehicle and was taken into custody for Felony Menacing and Driving Under the Influence of Alcohol. After receiving the information from the CIAC, the arresting officer believed the suspect in custody was also the suspect in the bookstore-bombing attempt. Concurrently, and while the investigation was still active, the CIAC received another lead from a different TLO which linked the suspect to yet another device that partially detonated near a hotel a short distance from the bookstore. The CIAC in turn passed this information to the FBI JTTF to further support the investigation, and the subject was arrested.

The JTTFs work across organizational boundaries on national terrorism issues. JTTFs, however, have a strict counterterrorism focus in contrast to State and local fusion centers' broader focus. JTTFs also conduct investigations as well as carrying out the "fusion" function of gathering information from multiple investigations to support analysis and situational awareness.

Nationwide Suspicious Activity Reporting Initiative

The FBI actively worked throughout 2012 to ensure Federal, State, local, and Tribal law enforcement agencies are aware of specific types of suspicious activities related to terrorism which they should report, and the process through which they should report this information. The FBI's unclassified eGuardian system is available to any law enforcement agency as a means to share terrorism-related Suspicious Activity Reports (SARs). This web-based system enables law enforcement agencies to input their own reports and run searches against other SARs. As a full participant in the Nationwide Suspicious Activity Reporting Initiative (NSI), the FBI and its eGuardian system serve as a means to enhance the reporting and sharing of terrorism-related suspicious activity reports. The FBI Counterterrorism Division's (CTD) Guardian Management Unit (GMU) is working closely with the NSI to facilitate an automated technological solution to share all Information Sharing Environment (ISE) SARs from the NSI Shared Spaces with eGuardian. The FBI publishes threat information assessments, intelligence notes, and other analytic products to the eGuardian site to broaden information sharing with law enforcement agencies and fusion centers utilizing eGuardian.

The FBI is working with the NSI to enhance sensitive but unclassified information sharing among all mission partners to protect the security of the nation. This initiative helps formalize the information sharing processes presently taking place among Federal, State, local, and Tribal partners, and leverages the already successful relationships between the partners and the FBI's JTTFs. In mid-2012, the NSI named the FBI to be the lead on all non-DHS Federal outreach. To date, the GMU has provided a total of eight Federal NSI/SAR Analyst training sessions to 74 individuals representing 28 separate Federal organizations.

Most noteworthy in 2012 was a dramatic increase in the number of terrorism-related SARs that were uploaded from State and local fusion centers into eGuardian. eGuardian also completed a new Privacy Impact Assessment (PIA) at the end of 2012 to allow it to collect cyber and other criminal information as well.

Law Enforcement Online (LEO)

The FBI's LEO system provides secure, web-based communications accessible via the Internet and is available to international, Federal, State, local, and Tribal law enforcement agencies. LEO enables the expedient sharing of sensitive information via professional special interest groups or topically focused dialogue, and provides access to an extensive array of FBI and other law enforcement agency databases and services. LEO gives law enforcement officers around the country access to unclassified information, intelligence reports, and alerts. It is interactive and provides state-of-the-art functions such as real-time chat capability, news groups, distance learning, and articles on law enforcement issues. LEO also offers a real-time electronic command center known as the Virtual Command Center (VCC) for information sharing and crisis/incident management accessible at local and remote sites.

The new LEO Enterprise Portal (LEO-EP) provides access to resources beneficial to the law enforcement community using single sign-on technology. That means users can log onto one authorized Identity Provider (such as a State or local police network) and automatically gain access to the LEO-EP homepage. The homepage is personalized for each user and includes links to services that the user is authorized to access. Current services include the N-DEx, the Joint Automated Booking System, the National Gang Intelligence Center (NGIC), the Internet Crime Complaint Center, as well as many others. OGC's PCLU embedded attorney at Criminal Justice Information Services Division (CJIS) worked closely to draft policy, implementation, and governance documents for the Portal to ensure that the data users and data providers would be following the FBI's security and privacy reviews. The Memorandums Of Understanding (MOUs) and other agreements for the service providers to sit on the Portal were also reviewed by the PCLU attorney.

LEO offers a variety of services to the criminal justice community that facilitate collaboration and cooperation among Federal, State, local and Tribal law enforcement personnel. Several accomplishments in 2012 enhanced the users' experience.

- Users saw significant changes to the appearance and functionality of the LEO system as a technical refresh was completed. These changes included: (1) upgrade of the LEO network support hardware; (2) use of a new e-mail application; (3) use of a chat feature; (4) the development of a content management system which made documentation location easier; and (5) new calendar functionality.
- The technical refresh integrated LEO services onto the LEO-EP.
- Four new identity providers—FBI Unclassified Network, the Texas Department of Public Safety, the U.S. Department of Justice myFX, and FBI National Crime Information Center Mobility—were on-boarded to the LEO-EP.
- LEO members created 390 new VCCs in 2012 and opened 728 VCC new event boards to collect, record, and disseminate information during numerous events.
    - In June, the FBI used three VCCs in Operation Cross Country VI, which spanned 57 cities and resulted in the recovery of 79 child victims of prostitution and the arrests of more than 100 criminals. More than 8,500 local, State, and Federal law enforcement officers, representing over 414 agencies, along with the National Center for Missing and Exploited Children partnered with the FBI for the operation. The VCCs were used to

track arrests and the recovery of victims, and provided nationwide situational awareness during the 3-day operation.

- LEO created a new, updated, user-friendly look with Virtual Offices (VOs). VOs can be used in a wide variety of law enforcement and emergency situations to strengthen counterterrorism, safety, and local and multi-agency law enforcement efforts. VOs have currently been created for FBI Special Agents, Drug Enforcement Agency Special Agents, U.S. Marshals Service Deputies and Task Force Agents, and many others.
- LEO members shared over 60,700 unclassified criminal activity and intelligence documents in 2012.

With more than 58,800 active members, LEO continues to succeed because it evolves as law enforcement's needs evolve—from offering training support to expanding and improving the individual sites that comprise the system. The LEO and LEO-EP systems are presently in a transitional phase which will be completed in 2013. Planned improvements include federated address book, mobile capabilities, enhanced vetting abilities, and exposing LEO email as its own separate enterprise service.

National Data Exchange (N-DEx)

The FBI CJIS Division's National Data Exchange (N-DEx), is the first and only national investigative information sharing system. N-DEx provides criminal justice agencies with a mechanism for sharing, searching, linking, and analyzing criminal justice information across the United States including incident, arrest, booking, incarceration, probation, and parole reports. N-DEx enhances the criminal justice community's ability to share relevant information in a timely and secure manner.

Thanks to system enhancements in Sentinel, the FBI's next-generation records management system, beginning in November 2012, the FBI standardized sharing its data in near-real-time to its criminal justice partners via N-DEx. All operational divisions within the FBI now share data via N-DEx—Counterintelligence, Criminal, Cyber, and Weapons of Mass Destruction Directorate. The FBI is sharing its investigative information with its criminal justice partners via N-DEx by contributing eligible new records essentially as soon as they are created.

State and local law enforcement agencies serving over fifty percent of the United States population contribute data to N-DEx. By the end of 2013, coverage is expected to expand to nearly sixty percent.

By using N-DEx as a pointer and data discovery system, users can detect relationships between people, events, property, and locations; eliminate information gaps by linking information across jurisdictions; "connect the dots" between non-obvious and seemingly unrelated data; and learn of investigators and agencies working similar investigations.

The goal was to provide investigators with records from the full criminal justice lifecycle—from arrest, to incarceration, to probation and parole. All of this shared information allows investigators to generate leads, solve crimes, eliminate information gaps across jurisdictions, deconflict investigations, identify victims, and help identify victim losses.

N-DEx Success Story

During a homicide investigation, a Hood River County, Oregon, Sheriff's Office Detective determined that the suspects lived out of state. Using N-DEx, the detective discovered records from the Los Angeles County, California, Sheriff's Department (LASD) containing information on the suspects, including information on several associates residing in California. Coordinating with the LASD Detective listed as the point-of-contact in one of the records, the Hood River County Detective was eventually able to develop the case to the degree that one of the suspects could be arrested in California. Thereafter, the detective was able to interview the suspect in Los Angeles and obtained additional information important to the case.

Three convictions resulted from this case. The shooter in the case was convicted of aggravated murder and received a sentence of 37 years to life. The two female accomplices were charged with homicide, but agreed to testify against the shooter and received sentences of Robbery 1st degree, which carried a sentence of 8½ years.

The Hood River County Sheriff's Office Detective in this case credits N-DEx with helping him solve the case. He had very little information to go on at the start of the investigation, but N-DEx put him in contact with detectives from another State who had key information regarding the suspect.

As of the end of 2012, over 70,000 total users had access to the N-DEx system. Approximately 4,000 agencies were submitting data containing over 150 million searchable records representing more than one billion entities (persons, places, things, and events). N-DEx continually strives to provide the criminal justice community with even more relevant investigative information. In 2012 CJIS expanded the N-DEx system to include records and users from corrections, probation, parole, courts, and prosecuting attorney's offices. The Indiana Department of Correction (DOC) began to submit its incarceration records in July 2012, making it the first DOC agency in the United States to share its investigative information via N-DEx. Kansas and Nebraska DOCs also began submitting data during 2012.

In 2012 N-DEx users gained access to 38 million records from the Department of Homeland Security and records from the Arizona Attorney General Southwest Border Anti-money Laundering Alliance.

Engagement with State and Local Fusion Centers

The Office of Partner Engagement (OPE) within the FBI's DI has program management responsibility for the FBI's engagement with State and local fusion centers. The OPE supports communication, coordination, and cooperative efforts between Federal, State, local, and Tribal law enforcement by providing varying levels of support to fusion centers throughout the United States. Fusion centers serve as the analytical hubs for their respective State and local jurisdictions and support the exchange of information and intelligence among law enforcement, public safety agencies, and private sector entities at the Federal, State, and local levels.

FBI Field Intelligence Groups (FIGs) are the focal point of the FBI Intelligence Program and are the logical conduit for information sharing and collaboration between the FBI (including the JTTFs) and fusion centers. Because fusion centers are often positioned to align with FBI priorities and programs, it is vital that the FBI and fusion centers have established partnerships to ensure the timely sharing of information addressing overlapping mission priorities, with an added emphasis on terrorism-related threat

information. Information sharing is enhanced through the deployment of resources (personnel and systems) to the fusion centers.

In 2012 the FBI, informed by the Information Sharing Environment's (ISE) Resource Allocation Criteria, developed a personnel resource allocation plan to place more Intelligence Analysts into fusion centers. Currently the FBI has 96 full and part-time personnel assigned to 55 fusion centers, 11 of which are co-located with the FBI. FBI systems are deployed to 49 fusion centers, with funding allocated for installation in five additional centers next year. In addition to resource contributions, the FBI has enhanced information sharing with fusion centers through the Nationwide SAR Initiative, the FBI Fusion Center Directors Orientation Program, increased dissemination of joint products, and continued partnership with the DHS State and Local Program Office (SLPO).

Tribal and Border Communities

Tribal governments and law enforcement agencies continued to work with the FBI to counter crime through participation in joint investigative efforts, liaison programs, and initiatives such as the FBI-led Safe Trails Task Force (STTF). The STTF unites Federal, State, local, and Tribal law enforcement agencies to combat crime and enhance information sharing practices in Indian Country. There are fifteen active STTFs. The FBI also has over 100 Special Agents working in support of Indian Country investigations. The FBI has multiple other avenues of outreach to State, local, and Tribal agencies, including those along the northern and southern borders. These include the JTTFs, formal liaison programs, LEO, eGuardian, N-DEx, and FIGs. The FBI's participation and leadership in multi-agency operations such as the Terrorist Screening Center (TSC), NCTC, ITACG, High Intensity Drug Trafficking Areas (HIDTA) Program, Organized Crime Drug Enforcement Task Forces, El Paso Intelligence Center, Port Area Maritime Security Committees, and Joint Interagency Drug Task Forces are also effective venues for outreach to local and Tribal agencies.

The most effective and productive interaction though, often comes through informal contacts and the establishment of personal and professional relationships between Agents and analysts in the field and their Federal, State, local and Tribal counterparts. Activities that support non-counterterrorism focus mission areas generate information highly relevant to border issues. This information flows through networks connected to those issues—including through FBI border liaison Agents, Regional Intelligence Groups (RIGs), and other FBI networks. Since not all local agencies have the ability to communicate via secure electronic means, face-to-face meetings and telecommunications between trusted partners are critical. This is especially true with respect to the Tribal areas and with border issues. The FBI also participates in ad hoc working groups throughout the nation (as well as on the borders) that develop information relevant to border issues. For instance, information developed regarding gangs and criminal networks frequently intersect with human smuggling or other border community issues. This information flows through appropriate law enforcement channels.

Cyber Information Sharing

In recent years the threat posed by terrorists, nation-states and non-state actors, and criminal groups conducting computer network operations against the United States has evolved into a top national security threat. Significant cyber incidents are now commonplace, occur at any time, and often impact more than one field office territory and operational division.

The FBI's cyber responsibilities flow from its role as both the nation's principal law enforcement agency and its domestic intelligence agency. Cyber incidents resulting from the malicious behavior of threat actors require a response by the FBI. For the purpose of informing the FBI's efforts, a cyber incident is defined as:

> The outcome of an action taken by an adversary targeting computers and networks to impair the confidentiality, integrity, or availability of data or networked services resulting in a threat to public health or safety, undermining of public confidence, harm to the economy, or diminution of the nation's security posture.

Next Generation Cyber (NGC) is an enterprise-wide initiative to strengthen the FBI's ability to combat cyber threats and adapt to rapidly evolving technology. NGC will enhance the FBI's role in investigating and countering threats to the nation's cybersecurity. The OGC and PCLU continue to provide legal support and guidance to ensure an adequate balance of investigative and privacy needs as this program grows. NGC implementation will enable the FBI to respond to significant cyber incidents.

- CyWatch: Cyber incident response requires complete and continuing situational awareness and effective national command and control of cyber intrusion incidents. As cyber incidents routinely occur during all hours, the FBI has established a cyber watch component called *CyWatch*. CyWatch is staffed 24/7 with a Cyber Program Supervisory Special Agent (SSA) and an Intelligence Analyst (IA). CyWatch maintains situational awareness of ongoing cyber incidents, and tasks and provides deconfliction regarding the FBI's response to new incidents. CyWatch works closely with the other Federal cyber centers including constant phone and message coordination.

- Cyber Task Forces: The FBI has established Cyber Task Forces (CTFs) in all 56 field offices to focus exclusively on cyber-security intrusion threats. In addition to key State and local law enforcement agencies, each CTF partners with many of the Federal agencies that participate at the headquarters-level in the FBI-enabled National Cyber Investigative Joint Task Force. These partnerships promote effective collaboration and deconfliction of efforts at both the national and local-level in responding to significant cyber incidents.

- Guardian: The FBI is expanding the capabilities of the Guardian system to support the Cyber Program's incident response efforts. When the upgrades are complete, Guardian will become the centralized incident reporting system for cyber incidents. These upgrades were completed and operational by January 1, 2013.

Sharing Efforts Directed Against Drugs, Gangs, and Other Crimes

The FBI continued to lead and work in task forces and operations centers with law enforcement and other agencies from all levels of government to cooperatively assimilate information and tackle the often inter-related crimes linked to drug trafficking, gangs, corruption, and violent crimes—including terrorism. In 2012 the FBI expanded information sharing and collaboration with U.S. Intelligence Community (IC) partners to mitigate cross-programmatic threats posed by transnational criminal enterprises and referred more cases to the NJTTF and local JTTFs.

The FBI strengthened its efforts with HIDTA by assigning two SSAs as liaison officers to the Office of National Drug Control Policy. Through these liaison officers, the FBI increased its collaboration with HIDTA partners to formalize information requirements and processes, and to incorporate them into a national threat information network. Like the FBI, HIDTAs are finding that information developed through their traditional operational roles increasingly overlaps with information developed for national security missions. The FBI liaison officers held meetings to share information regarding gaps in intelligence sharing between HIDTAs and Indian Country law enforcement and collaborated to have more HIDTA involvement to close those gaps.

The NGIC is the only Department of Justice entity tasked with collecting, analyzing, and disseminating gang intelligence products to support Federal, State, local and Tribal law enforcement agencies in their efforts to disrupt and dismantle the gangs that continue to pose a threat to communities throughout the United States. On a daily basis, the NGIC assists with regional and national threat assessments; geo-spatial analysis projects; identification of gang signs, symbols, and tattoos; and analytical support for specific gang-related investigations.

The NGIC developed NGIC Online to assist in meeting its missions. NGIC Online is a web-based tool designed for researching gang-related intelligence. The system is a free resource available to law enforcement throughout the United States. It is accessible through LEO as well as the Regional Information Sharing System Network for sworn law enforcement users.

NGIC Online allows law enforcement members to search the system's library of intelligence products and symbol and tattoo images, and to post announcements, officer safety reports, and requests for information. The system also contains an anti-gang training and events calendar, discussion board, and a searchable dictionary of gang terms.

In addition to NGIC Online, gang intelligence is exploited and shared through a unique partnership between the NGIC, the FBI's Safe Streets Gang Unit, and the California Department of Corrections and Rehabilitation. This partnership led to the creation of the California Gang Intelligence Initiative (CGII). The CGII uses the NGIC Online interface to exploit and disseminate prison gang intelligence nationwide.

Other Administrative Actions to Improve Sharing and Safeguarding

Effective and efficient sharing and safeguarding requires a clear understanding of the information itself, its sensitivity, and value. The FBI's Security Division supports information sharing efforts through an enterprise-wide commitment to training and education. In 2012 the Security Division/Mission Support Section/Information Security Team trained over 4,600 employees—from new Special Agents to legal attachés—on identifying, designating, and marking classified information. Additionally, a web-based training module was developed for the same training, placing comprehensive classification and marking guidance at the fingertips of every employee. All individuals with access to FBI systems/information are also required to take privacy training within a certain timeframe and receive annual updates in the web-based information security training.

D. Leveraging the Capabilities of Partners

The FBI continues to rely on the inherent capabilities of mission partners in multiple different communities to gather and share information in support of common missions. Through continued

engagement, the FBI seeks not only to improve information acquisition, but also to leverage partner capabilities to mitigate threats to people and infrastructure.

Terrorist Watchlisting and Screening Communities

The FBI fills a strong leadership role in the Watchlisting and Screening Community, notably through its management of the TSC, as well as through representation on various national-level policy, law enforcement, and intelligence committees. Relationships developed through these roles, and decades of investigative experience, are critical to ensuring continued open dialogue, business process, and information sharing enhancements among the partners. Due to trust and standardized processes, law enforcement encounter data is now being provided to counterterrorism analysts and processed daily in a secure manner for sharing with the broader IC. The FBI's role in multiple related efforts in law enforcement helps ensure that technology or techniques developed in one arena can be readily recognized as applicable to IC and counterterrorism analysis while protecting privacy and civil liberties. (More specific information about the TSC is provided in Section IV.)

Biometrics

Through the CJIS Division's interoperability initiatives, the FBI and other government agencies can more effectively and efficiently exercise national security responsibilities. Combining the search power of the FBI's Integrated Automated Fingerprint Identification System (IAFIS) with the biometric databases of local, State, Tribal, Federal, and international partners enables a more comprehensive use of key resources to identify criminals and terrorists. At the CJIS Division, advances in biometric interoperability have been developed through continued information sharing between the FBI, DHS, DOS, and the Department of Defense (DoD). These partnerships, reflected in an Interoperability Privacy Impact Assessment, have provided the FBI and its stakeholders increased access to the DHS's Automated Biometric Identification System (IDENT) and the DoD's Automated Biometric Identification System (ABIS), enabling successful identification and exchange of information on criminals who might otherwise have been missed. These technological advances have also incorporated capabilities to ensure that the privacy and civil liberties of U.S. Persons remain protected. Because the FBI's technological capabilities in biometrics continue to develop, the PCLU and other OGC units work closely with CJIS to ensure that the FBI's privacy and civil liberties protection policies keep pace with new scientific advancements.

Search capability of the full DHS IDENT repository is now available to State and local law enforcement within all 50 States, the District of Columbia, and four U.S. Territories. This repository includes Tribal and Federal agency submissions through State identification bureaus. Federal agencies submitting criminal answer-required transactions are now directly searching IDENT. Such searches include criminal answer-required transactions coming from tribal agencies through the Bureau of Indian Affairs.

The DoD Special Operations Command can also submit transactions through CJIS for searches of IDENT. These transactions will continue to come through CJIS until a direct connection is established between ABIS and IDENT.

The CJIS Division has teamed with the DoD and the Texas Department of Public Safety (TXDPS) to implement a latent print interoperability pilot. The pilot provides the TXDPS the capability to submit latent prints through the IAFIS and choose to search the latent prints against IAFIS or ABIS, or both, with a single request.

Private Sector Stakeholders

The FBI continues to develop and enhance effective and efficient information sharing partnerships with the private sector. While ensuring that all proprietary information is protected to the extent possible, the FBI shares information on incidents, threats, consequences, and vulnerabilities, as appropriate. Operational programs (Counterintelligence, Counterterrorism, Criminal, Cyber, and Weapons of Mass Destruction) and Community Outreach have continuing efforts to engage with the private sector to build partnerships and to increase awareness. With OGC support, the FBI leverages the capabilities of these partners through programs like DSAC, InfraGard, and other programs and initiatives described below.

Domestic Security Alliance Council (DSAC)

The DSAC, a strategic partnership between the FBI, DHS, and the U.S. private sector, was established to promote the timely and effective exchange of information. The DSAC advances the FBI mission of preventing, detecting, and investigating criminal acts, particularly those affecting interstate commerce, while enhancing the ability of the private sector to protect its employees, assets, and proprietary information.

InfraGard

InfraGard is a partnership between the FBI, State and local law enforcement agencies, academic institutions, an association of businesses, and other organizations dedicated to protecting the United States' critical infrastructure by sharing information regarding both cyber and physical threats and vulnerabilities. The goal of InfraGard is to promote an ongoing dialogue and timely communication between its members and the FBI for investigative and intelligence gathering purposes. Since its founding in 1996, InfraGard has helped to establish a relationship of trust and credibility between the private sector and the FBI regarding the exchange of terrorism, criminal, and security information and intelligence.

The FBI provides information to InfraGard members in the form of alerts and advisories via secure email and a secure website. InfraGard members share information with the FBI and with each other by posting articles on the secure website and online bulletin boards, as well as via secure email, list servers, and networking at membership meetings. InfraGard chapters are linked with FBI field office territories and are assigned an FBI Special Agent Coordinator. The FBI Coordinator also works closely with SSA Program Managers in the Cyber Division at FBI Headquarters.

Cyber Initiative Resource Fusion Unit

The Cyber Initiative Resource Fusion Unit is an FBI Cyber Division unit embedded at the National Cyber Forensics and Training Alliance (NCFTA), a non-profit corporation located in Pittsburgh, Pennsylvania. The NCFTA is a fusion center combining law enforcement expertise with academia and the private sector. Experts from Federal agencies, universities, Internet security companies, Internet service providers, the telecommunications sector, and the financial sector share information and collaborate on security breaches, as well as identifying current and emerging cyber threats.

Counterintelligence Strategic Partnership Initiatives

The FBI's Counterintelligence Strategic Partnership Unit and the Strategic Partnership Coordinator in each FBI Field Office collaborate with key private sector stakeholders on critical technology targeted by

foreign adversaries. This collaboration fosters communication and builds awareness with key academic, business, and strategic entities, and educates and enables the partners to identify assets that are at counterintelligence risk and how to better protect them. The FBI calls this "knowing your domain," identifying the research, information, and technologies that are targeted by foreign adversaries, and establishing an ongoing dialog and information exchange between partners to change detrimental behaviors and reduce opportunities that benefit the opposition. The FBI participates in a number of national-level efforts to establish and maintain sharing relationships to protect U.S. business interests, with both the IC and private sector partners.

- The Counterintelligence Business Alliance protects U.S. interests being targeted by foreign intelligence services by developing partnerships with private sector entities, at both the corporate headquarters and the local office levels, that result in bi-directional sharing of relevant and actionable information. The National Security Business Alliance Council (NSBAC), the national-level business alliance umbrella organization, is a partnership with leading companies in the defense industrial base and the telecommunications sector that are the stakeholders of key technologies targeted by foreign adversaries.

- The Counterintelligence Academic Alliance's mission is to effectively and actively engage the IC with college and university leadership throughout the United States to raise national security awareness. The National Security Higher Education Advisory Board (NSHEAB) emphasizes relationships between the FBI and select college and university presidents and chancellors. This program promotes information sharing and sustained relationship building among the academic institutions, the FBI, and the IC.

- The National Counterintelligence Working Group (NCIWG) establishes ongoing interagency discussions of counterintelligence policy and operational issues and initiatives. The NCIWG is led by the Assistant Director of the Counterintelligence Division (CD), and consists of counterintelligence executive representatives from more than 45 IC, law enforcement, and U.S. government agencies, as well as the defense industrial base and the academic community represented by the Chairman of the National Security Higher Education Advisory Board (NSHEAB).

- The Counterintelligence Threat Working Group (CITWG) facilitates execution of the FBI's national counterintelligence strategy in collaboration and coordination with IC partners by focusing on the prioritized threats to national security. Recognizing that IC issues transcend the FBI's divisional boundaries, the CITWG affords a perspective that reaches across the United States and links FBI field offices and IC partners that focus on a common national security threat, regardless of geographic location. The CITWG concept encourages the establishment of partnerships within the FBI, with other government agencies, and with cleared private sector entities from the defense contractor and academic communities.

United States Oil and Natural Gas Crime Issues Special Interest Group

The United States Oil and Natural Gas (USONG) Crime Issues Special Interest Group (SIG), is a strategic partnership established to promote the timely and effective exchange of information between the FBI and the U.S. oil and natural gas private sector. The USONG SIG is unlike other FBI private sector outreach programs in that it is specific to one national critical infrastructure industry. In order to provide streamlined and timely information to our partners, the USONG SIG regularly coordinates with other outreach programs including the DSAC, InfraGard, the Counterintelligence Strategic Partnership Coordinators, and the Intellectual Property Rights Center. The USONG SIG believes it is crucial that law enforcement at the State, local, Tribal, and Federal levels be able to share information collected and analyzed across their regions. In addition, the FBI's private sector partners require access to threat information so they can mitigate existing vulnerabilities. To facilitate this information flow, the USONG SIG has developed a SIG on LEO. This allows for secured communications between the oil and natural gas sector and law enforcement at all levels. This LEO SIG allows information sharing, meetings, and coordination to take place independent of geographic location. This collaborative ability is especially important given that many locations where oil and natural gas exploitation takes place are located in less populated areas, including Tribal reservations and Tribal-owned land. The USONG SIG also works with ad hoc working groups across the United States to continue to promote face-to-face meetings and to provide the LEO SIG as a secure venue for communications between working group members.

Sharing with International Partners

The FBI regularly shares unclassified and classified information with foreign governments as part of its authorized law enforcement, national security, and intelligence missions. Sharing with foreign partners, including the exchange of biographic and biometric information regarding known or suspected terrorists, requires both flexibility and appropriate security precautions. The FBI strictly adheres to necessary handling restrictions and ensures the protection of U.S. persons' data.

The FBI's International Operations Division (IOD) administers the Legal Attaché (Legat) Program, the foundation of the FBI's international program. IOD's role is to support the FBI's mission to defeat national security and criminal threats by building a global network of trusted partners and strengthening international capabilities. The FBI has Legat offices and suboffices in 78 key cities around the world, providing coverage for more than 200 countries, territories, and islands. In direct consequence of their relationships with law enforcement and intelligence services abroad, Legats are familiar with investigative rules, protocols, and practices that differ from country to country. They are thus well-positioned to analyze and disseminate the intelligence that directly impacts U.S. national interests both domestically and abroad. Through international liaison and overseas operations, the IOD and the Legat program disseminate more intelligence information reports to the IC than the next highest producing field divisions combined.

In August 2012, the IOD published the International Operations Division Corporate Policy Directive and Policy Implementation Guide, which outlines policies and procedures for conducting extraterritorial FBI operations. These guidance documents also include policies and guidance for retention and sharing of information and sharing with foreign partners.

Strategic Alliance Group (SAG)

The FBI participates in the SAG, a multi-national law enforcement instrument focused on international criminal issues, including cyber-enabled crime, criminal groups, and financial crimes. The group's members consist of representatives from the national law enforcement agencies of Australia, Canada, New Zealand, the United Kingdom, and the United States. The SAG members exchange information, discuss emerging threats, and collaborate on training.

IV. Maximizing and Integrating Information Sharing Capabilities

The FBI continues to refine its processes for collecting, analyzing, and sharing information through improvement of its discovery, access, and collaboration capabilities. FBI operational divisions and other intelligence and law enforcement agencies provide the information, and technology enables the FBI and its partners to find patterns and connections to drive operations.

A. Discover, Access, and Exploit Information Based on Mission Need

Sentinel

In July 2012 the FBI deployed Sentinel, the FBI's electronic case management system, which greatly advanced making information available to the IC and Federal, State, local, Territorial, and Tribal law enforcement agencies. With 27 interfaces to legacy, stove-piped systems both internal and external to the FBI, Sentinel provides its users with timely, accurate, and cost effective data sharing services; and grants special access to approved Task Force Officers (TFOs). An important goal of Sentinel is to increase efficiency, address the data needs of IC and law enforcement partners, minimize data replication, and increase the integrity and security of FBI case data.

In support of the Criminal Justice Community and consistent with OGC guidance, Sentinel shares information with N-DEx, providing missing information links and fostering the development of partnerships that lead to more effective investigations. To further the FBI's progress in protecting the United States from espionage and counterterrorism, Sentinel shares data with the National Name Check Program, which is used by Federal agencies; components within the Legislative, Judicial and Executive branches of the Federal Government; certain foreign police and intelligence agencies; and State and local law enforcement agencies. In the FBI's continuing support of the U.S. Government's counter-drug mission, Sentinel provides important drug-related data to the Department of Justice (DOJ), Treasury Department, and DHS through its interface with the Organized Crime Drug Enforcement Task Force system. In addition, Sentinel shares data with Delta, the FBI's confidential human source management tool; eSubpoena, an administrative subpoena tracking tool; the FBI Intelligence Information Report Dissemination System; the Foreign Intelligence Surveillance Act Management System; Foreign Terrorism Tracking Task Force (FTTTF) Data Mart; Guardian, the FBI's counterterrorism threats and suspicious activities reporting tool; the NGIC information system; Operational Response and Investigative Online Network (ORION), the FBI's Crisis Case system; the Surveillance Program Integrated Reporting and Intelligence Tool; and the Victim Notification System.

In continued support of internal FBI information sharing initiatives, Sentinel assists FBI Agents and intelligence analysts in performing critical analytical activities by sharing data with the Data Integration and Visualization System (DIVS), and streamlines U.S. Attorney data gathering activities with an electronic export function. Sentinel provides FBI executive management and field office leadership with operational and institutional information through tools such as Compass, the FBI's tool to manage people and resources; the FBI Automated Messaging System, a tool for Agents and analysts to access messages released by CIA, DOS, DHS, and other Federal agencies throughout the IC; the Clearance Processing System, to track background investigations; and *Quickhire*, for managing new hire vacancy announcements.

Data Integration and Visualization System (DIVS)

The DIVS efficiently facilitates the sharing of information, from both internal and external data sources, vital to FBI personnel to support research, analysis, and investigation. The DIVS provides a single interface that Agents and analysts can use to search multiple FBI data repositories, filter results, and quickly locate information most relevant to their needs. The DIVS was created to enable users to effectively and efficiently search and prioritize data.

Next Generation Identification System

In 2012, the CJIS Division, using new technologies, continued to enhance the FBI's ability to more quickly and accurately identify criminals and terrorists. The Next Generation Identification (NGI) system is incrementally replacing the IAFIS, which provides automated fingerprint and latent search capabilities to more than 18,000 law enforcement and criminal justice partners, increasing the accuracy of fingerprint searches from 92.0 to 99.6 percent. As NGI is implemented, a PCLU attorney completes Privacy Impact Assessments for each significant development and an NGI System of Records Notice is published. A PCLU attorney has worked closely with NGI during the entire development process and has been an integral part of the technical, policy, and legal decision making regarding the FBI's largest biometric system.

Additionally, the NGI system continues to grow the user base for its new Repository for Individuals of Special Concern Rapid Search capability. This service provides law enforcement personnel using mobile fingerprint devices access to a highly actionable subset of wanted persons, known and suspected terrorists, sex offenders, and other persons of special interest. Also in 2012, the NGI program deployed the Interstate Photo System Facial Recognition Pilot, providing search and facial recognition capability of photographs found in a national repository of more than 13 million criminal mug shot photographs. Appropriate privacy documentation for the Interstate Photo System has been drafted, under the supervision of a PCLU attorney.

B. Enhance Capabilities for Collaboration and Information Sharing

Biometric Center of Excellence

The Biometric Center of Excellence (BCOE), created in 2007, supports the FBI's overall biometrics mission, major programs, and strategic initiatives that comprise the FBI's biometric services. The BCOE explores and advances new and enhanced biometric technologies and capabilities for inclusion into FBI operations. The BCOE leverages the skill and expertise of FBI staff from across the Science and Technology Branch including the CJIS Division, the Laboratory Division (LD), and the Operational Technology Division (OTD), plus the OGC's Science and Technologies Section and the PCLU. In 2012 the BCOE sponsored 30 applied biometric research projects to further the field of biometrics while sponsoring 10 collaborative events fostering biometric discussion and development. The BCOE is a vital biometrics facilitator and collaborator, helping the FBI assist its partners by advancing biometrics and related identity management technologies.

During 2012 the BCOE led several interagency collaborations in advancing facial recognition technology. One such collaborative endeavor was the U.S. Government Facial Recognition Legal Series (Legal Series). The Legal Series was comprised of four interagency legal and policy forums specific to facial recognition. It brought together lawyers, policy experts, technical personnel, and biometric program

managers from nearly 40 Federal law enforcement and homeland security agencies, the military, and the IC to discuss the legal and policy challenges of facial recognition. Topics included interagency information sharing challenges, best practices, privacy and civil liberty considerations regarding facial recognition deployment, and public perception as a critical factor in effective policy development. As a result of the BCOE's recommendations following the Legal Series, the National Science and Technology Council is developing guidelines to be used by Federal agencies to construct facial recognition technology policy.

In 2012 the BCOE team also successfully transitioned the management of the Rapid Deoxyribonucleic Acid (R-DNA) initiative to the FBI's Laboratory Division (LD). The BCOE, in collaboration with the DOS and DHS, has been expanding capabilities to bring advanced DNA analysis to law enforcement by sponsoring the development of portable R-DNA devices that will quickly process DNA at booking stations. Through the BCOE's collaborations, three mobile R-DNA devices were developed with the goal of analyzing DNA in less than 90 minutes, searching the FBI's National DNA Index System using enhanced Combined DNA Index System software, and being able to be operated outside of a laboratory environment with minimal user training.

Initial testing revealed that the devices were capable of processing DNA within the targeted timeframe while achieving high success rates. The devices processed samples in significantly less time than traditional laboratory techniques, which often require two or more days utilizing multiple instruments, separate rooms, and numerous complex steps. The devices will continue to undergo additional testing in the FBI's LD with the goal of becoming field deployable units available to private and government laboratories and law enforcement and national security personnel. This technology can enable law enforcement to quickly determine if a subject in custody may be linked to another crime, and will also allow for a more efficient and less costly analysis. Furthermore, the R-DNA devices utilized within crime laboratories will enable forensic scientists to dedicate a greater amount of time to other case work.

Through the BCOE's partnership with Michigan State University, the BCOE developed the TattooID prototype for the automated retrieval, indexing, and matching of scars, marks, and tattoos. The TattooID allows for searches of tattoo images, key words, or characters to find similar images. Although search results do not provide positive identifications at this point, the results can help narrow suspect lists, determine gang associations or activity, and potentially help link gang crimes throughout the United States. The BCOE also developed a tattoo dataset to test and evaluate the image-matching algorithms in the prototype.

Biometrics continues to be an invaluable technology for solving and preventing crime. The BCOE will continue to collaborate with stakeholders, build partnerships, and leverage resources to advance the field of biometrics and provide solutions to operational challenges. The OGC and PCLU are keenly aware that technological advances may bring new and increased risk to privacy and civil liberties, and continue to work with BCOE to craft appropriate policies to mitigate these risks.

The eGuardian System and Suspicious Activity Reporting

The FBI's Counterterrorism Division's Guardian Management Unit (GMU) continues to support the unclassified version of its Guardian program. This information sharing platform, called eGuardian, was developed to help meet the challenges of collecting and sharing information about potential terrorism

related activities with law enforcement agencies across various jurisdictions. Accessible via LEO, the system facilitates situational awareness of suspicious activities, threats, and events with a potential nexus to terrorism and cyber threats, allowing law enforcement agencies to combine new SARs along with existing legacy and NSI SAR reporting to form a single information repository accessible to thousands of law enforcement personnel.

The eGuardian system is a valuable information sharing tool, assisting in law enforcement collaboration and threat mitigation. The information captured in eGuardian is also migrated to the FBI's internal Guardian system, where it is assigned to the appropriate FBI Field Office and assigned to the JTTF for further investigative actions. Interagency information sharing via eGuardian has proven to be very successful. Of all the incidents entered into eGuardian, approximately 6% have been converted to either preliminary or full investigations or have enhanced existing investigations.

The system was modified and improved in 2012 based on feedback and suggestions from users. Modifications were also made to facilitate better system and information incorporation into the NSI. The FBI modified its internal business processes in 2010 and has continued to push unclassified Guardian incidents to eGuardian, ensuring full FBI participation in the eGuardian system and the broader NSI information sharing process. Over the past several years thousands of unclassified incidents have been pushed from Guardian to eGuardian and to the NSI Shared Spaces.

During 2012 the number of agencies and users of eGuardian continued to expand, including over 1,378 member agencies and organizations with approximately 4,200 active users. The FBI actively reaches out to, and provides training for, mission partners on the use of eGuardian and the importance of information sharing. In 2012, GMU provided 101 training and outreach opportunities to mission partners and other interested entities. Member agencies include local police and sheriffs' departments, State-level agencies and fusion centers, Tribal law enforcement, campus law enforcement, and other Federal agencies, including law enforcement components within the DoD. This training includes instruction from PCLU attorneys on privacy and civil liberties. In particular, the training emphasizes avoiding eGuardian reports that would constitute a violation of a person's civil liberties, such as by reporting activity that is in fact nothing more than an individual exercising his or her First Amendment rights.

Terrorist Screening Center (TSC)

In response to the terrorist attacks of September 11, 2001, the President signed Homeland Security Presidential Directive 6 (HSPD-6), directing the Attorney General to consolidate the U.S. Government's approach to terrorism screening, and to provide for the appropriate and lawful use of terrorist identifiers in screening processes. It was recognized that for the watchlisting and screening community to achieve this objective, it would be necessary to establish and expand partnerships among all concerned agencies, take an integrated team approach, and facilitate communications by sharing information at appropriate classification levels. In accordance with HSPD-6, the TSC was created as a multi-agency center that incorporates assignees from across the watchlisting and screening community, including the DHS, DOS, FBI, and other national security agencies and organizations.

Before HSPD-6, various agencies maintained nearly a dozen separate watchlists designed to screen persons of interest to U.S. law enforcement and intelligence officials. There was no central clearinghouse where all law enforcement and government screeners could access the best information about a potential

person of interest. The TSC, which became operational in December 2003, addressed that issue through the consolidation of information relating to known and suspected terrorists (KST) into a single database. The TSC maintains the Terrorist Screening Database (TSDB), commonly referred to as the Terrorist Watchlist, the U.S. Government's consolidated watchlist for terrorist screening information.

The watchlisting community provides TSDB KST nominations through the National Counterterrorism Center (NCTC) for international terrorists and through the FBI for domestic terrorists. These nominations of KSTs are supported by a reasonable suspicion of their involvement in terrorist activity, as developed by the nominating agency. The TSC conducts over 1,000 unique database transactions daily that result in the addition, modification, or deletion of KST identities in the TSDB. It is through this expeditious and dynamic process that the TSC strives to maintain a thorough, accurate, and current database of KSTs for lawful and appropriate use in the screening process.

The TSC operates a 24/7/365 call center to assist authorities in determining whether individuals encountered during the terrorist screening process are a positive match to a KST watchlisted in the TSDB. Applicable portions of the TSDB are provided to law enforcement, intelligence, and other governmental partners that conduct daily screening operations. The screening process empowers thousands of law enforcement officers and other government workers to play an important role in efforts to identify KSTs and deter and prevent future terrorist attacks. Additionally, the TSC Outreach Team provides nationwide briefings and awareness training for police dispatchers, law enforcement officers, and other government officials, as well as web-based training to ensure all partners are informed on watchlisting and screening processes. During 2012 the TSC's Domestic Outreach Team trained over 15,000 participants.

The TSC works closely with all 78 fusion centers throughout the United States, notifying them whenever there is an encounter with a KST in their jurisdiction, as well as liaising with the National Fusion Center Association Executive Board and the Fusion Center Office at the DHS Office of Intelligence and Analysis. By working closely with the fusion centers and oversight organizations, the TSC ensures that the fusion center notification system continues to facilitate the accurate and timely dissemination of KST information.

In addition to its role in the terrorist watchlisting and screening process, the TSC annually provides hundreds of uniquely tailored intelligence and analytical products to its Federal, State, local, Tribal and Territorial partners. The TSC's Intelligence Office continually analyzes terrorist encounter data to identify significant trends and disseminates this information to interagency partners.

Protecting civil liberties is a cornerstone of the TSC's mission. The operating procedures used by the TSC to accurately process all watchlisting data, to expeditiously respond to terrorist screening encounters, and to promptly provide a redress mechanism to resolve watchlisting discrepancies are designed to facilitate the protection and safeguarding of civil liberties. The goal of the watchlist redress process is to provide for timely and fair review of individuals' complaints and to identify and submit corrections of any errors in the TSDB. In addition, the OGC/PCLU has a dedicated attorney embedded with TSC who helps provide privacy and civil liberties training and advice to TSC.

Since the TSC began operations, the TSDB has become the world's most comprehensive and widely shared repository of terrorist identities.

Next Generation Sensitive Compartmented Information Operational Network

The FBI made great progress with its Next Generation Sensitive Compartmented Information Operational Network (NGSCION) deployment and enhancements throughout 2012, upgrading capabilities for highly-sensitive information processing. By the end of 2012, more than 70 percent of all Sensitive Compartmented Information Operational Network (SCION) users had migrated to NGSCION.

Sensitive Compartmented Information Network (SCINet)

The FBI is the first IC member organization to provide an enterprise wide desktop-to-desktop secure voice capability for all FBI users of its SCINet computers. This capability also provides video, real time presence, VTC, desktop/program sharing, and instant messaging to all FBI users as needed. This project also includes a pilot project that enables the FBI intelligence worker to call most secure phone systems within the IC without the use of a STE or other secure phone instrument. Upon successful completion of the pilot project, the FBI will essentially have provided all SCINet users with a secure phone at their desk.

In addition to deploying NGSCION, the FBI provided a network environment that is not only more secure, reliable, and stable, but also more tailored to the needs of FBI users, in particular those Agents and analysts located in the FBI's Field Intelligence Groups. In 2012, enhancements were deployed on NGSCION that have a significant impact on collaboration and information sharing with the FBI's IC partners, including:

- Remote Access. NGSCION users can connect to the NGSCION Virtual Desktop from an external Top Secret (TS) workstation within the IC and access the same resources and functionality as if they were sitting at an FBI TS workstation.

- Desktop Video Teleconferencing (VTC). Conducted successful engineering and business pilots for desktop VTC on NGSCION using Microsoft® Lync. Planned deployment of desktop headsets and web cameras will enable NGSCION users to benefit from the audio and video conferencing and integrated online meeting functionality of Lync.

During 2013, the FBI expects to complete NGSCION deployment to the FOs, with the goals of retiring the legacy SCION and deploying desktop headsets and web cameras to NGSCION users. Enhancements for 2013 include completing the upgrade to Windows 7 and configuring current operational technologies such as Lync to communicate with our IC partners.

V. Maximizing and Integrating Capabilities to Secure Information

In 2012, the U.S. Government continued major efforts to identify information safeguarding weaknesses and vulnerabilities and to eliminate or mitigate them. The FBI's own internal efforts identified several measures critical to protecting the nation's network of information systems: interoperable identity management; user authorization and access; and auditing and monitoring to safeguard information, improve oversight, and protect information networks from external and insider threats. Initiatives already underway at the FBI for implementation on internal networks address some of these measures. Work began in other areas to address as yet unmet requirements.

A. Identity Management

The FBI has long been committed to implementing effective identity management capabilities—and closely related access management—across all its networks and systems. Staff worked closely with Federal partners throughout 2012 to advance development and implementation of Identity, Credential, and Access Management (ICAM) capabilities across Federal networks, to enable interoperability with FBI networks, and to promote information sharing, and efficiencies of scale across all agencies within the Federal Government.

The FBI uses Public-Key Infrastructure (PKI) digital certificates for network authentication and digital document signing for Secret enclave mission systems such as Sentinel and Delta, and for access to certain sites and applications on the Joint Worldwide Intelligence Communications System (JWICS). In 2012, FBI PKI certificates issued went from 30,000 to 40,000 subscribers for Secret Internet Protocol Router Network (SIPRnet) interagency email encryption and digital signing.

During 2012, the FBI continued to manage and maintain the Enterprise Directory Service (EDS), an integrated commercial off-the-shelf (COTS) solution, on its Secret enclave, FBINET. EDS is an automated directory for applications and certain privileged users that retrieves user identity attributes from a centralized service compiled from multiple authoritative sources for access control decisions. This solution has been running successfully for the past two years. In addition, the CJIS has built and installed the Trusted Broker which allows external users to federate into CJIS without using a name and password. This implementation of an enterprise identity and access management application meets ICAM standards.

The FBI is in the process of evaluating ICAM standards for its unclassified network and systems to determine how they would affect current systems and requirements. It is expected that this evaluation will be completed in 2013. If any of the FBI's service and identity providers adopt ICAM standards during the interim, the Bureau will accept these upgraded services and products based on the availability of funding and resources.

The FBI has identified and defined its requirements for an enterprise-level identity management solution for its classified systems and networks that will facilitate the adoption of ICAM standards. Development began and continued through 2012.

B. User Authorization and Access

The Office of Integrity and Compliance (OIC) conducts compliance-risk assessments which review FBI policies, procedures, training, and monitoring in specific areas to determine whether they are adequate to

mitigate any risk of non-compliance with governing law and regulation as the FBI executes its mission. OIC has conducted and continues to conduct such assessments in areas involving the sharing of information.

In November 2012 and with input from the OIC, the OCKO and the Enterprise Data Management Office began an effort to develop an enterprise data access rules registry and enterprise data access policy.

This initiative to develop and deliver the registry of access rules, and the concurrent efforts to develop and identify corresponding attributes and data labels, will proceed in phases until ultimately rules governing access to all FBI data are included. IT services will be developed to implement the Attribute-Based Access Control (ABAC) capability across FBI networks and systems.

C. Audit and Monitoring

The FBI has been a leader across the Federal Government in audit and monitoring. All FBI IT systems must now participate in (and are now migrating to) enterprise-level integrated system security monitoring. Specific audit and monitoring requirements are determined based on published standards related to the IT system's criticality to the FBI mission prior to being authorized on the FBI's computer networks. Work continues to enhance the FBI's ability to monitor all systems in the field as well as share audit information appropriately with external partners.

Throughout 2012, the FBI enhanced its internal policies, procedures, and accountability to decrease risk to sharing information in the FBI's classified networks as part of a long-term comprehensive enterprise Data Protection Program. The Security Division and Information and Technology Branch (ITB) expanded their systematic efforts to appropriately manage data transfer, minimize the use of removable electronic storage devices, and encourage the use of enterprise cross-domain solutions to enable responsible information sharing. This program supports audit and monitoring as well as the FBI's "insider threat" detection and monitoring program.

VI. Strengthening the Governance Framework

The FBI is committed to sharing timely, relevant, and actionable intelligence with its mission partners as part of its national security and law enforcement missions. These relationships are governed through both internal and external boards and committees, which collaborate to strengthen the framework to optimize responsible information sharing while protecting civil liberties and privacy.

The President's approval of the National Strategy for Information Sharing and Safeguarding in December 2012, reinforced the concept that policy and governance are critical to information safeguarding and secure sharing. The FBI participated in Interagency Policy Committees (IPCs) that affect the manner in which the Federal Government shares information. The Program Manager for the Information Sharing Environment (ISE) is the co-chair of one of those IPCs and ensures that State, local, Territorial, Tribal, and private sector equities are included in policy decisions associated with counterterrorism, weapons of mass destruction, and homeland security. The Office of the Director of National Intelligence (ODNI) sets ground rules for the sharing of sensitive intelligence among the members of the Intelligence Community, including the FBI. The Department of Justice assumed new roles, and continues to sponsor other initiatives that enhance FBI information sharing.

A. FBI Governance of Information Sharing

Information sharing is a critical part of all FBI missions, and is performed across the entire Bureau. Driven by the FBI mission to protect and defend, the ISPB is the FBI's primary authority for information and intelligence sharing policy. It is supported by the APG and Information Sharing Teams (ISTs). In November 2012, the Chief Knowledge Officer was named the Principal FBI Official for Information and Intelligence Sharing Policy, replacing the Executive Assistant Director (EAD) of the National Security Branch. The CISO is the dedicated FBI Senior Information Sharing Official required by Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," and also serves as the FBI representative on the Information Sharing and Access Interagency Policy Committee (ISA IPC). In November 2012, the CISO became a direct report to the FBI CKO. In turn, the OCKO was realigned to the Office of the Associate Deputy Director of the FBI, and the CKO assumed an increased Bureau-wide responsibility and authority including chair of the ISPB.

Information Sharing Policy Board

Director Robert S. Mueller III chartered the ISPB in 2005 to develop FBI policy for internal and interagency information sharing from an intelligence and operational mission perspective. By charter, the ISPB is chaired by the Principal FBI Official for Intelligence and Information Sharing Policy. Board membership consists of all EADs and Assistant Directors, the CKO, the FBI Senior Privacy Official, and the General Counsel. The ISPB's primary goal is to initiate, develop, enact, monitor, and maintain the policies, decisions, and relevant procedures to facilitate the FBI operational divisions' criminal and intelligence information sharing. The ISPB evaluates business practices that bear on information and intelligence sharing and provides policy direction to produce a mission-driven information exchange across all FBI components and external partners. Subsequent to E.O. 13587, the ISPB has served as the entity ensuring the FBI meets those mandates and principles. The CISO serves as Executive Secretary of the ISPB and acts as principal advisor on information sharing activities.

In 2012 the ISPB met five times. Activities covered these priorities:

- The OIC Information Access Compliance Analysis (the "Red Team");
- Cross-domain data transfer capabilities;
- NCTC ingest of International Terrorism Case files from Automated Case Support System (ACS), and later from Sentinel;
- Executive Order 13587 implementation and associated "structural reform" resource requirements;
- Greatly increasing the amount of investigative case material that will be shared with state, local, tribal, and territorial criminal justice organizations via N-DEx; and,
- Monitoring updates on information sharing activities in the interagency arena, especially preparing and finalizing the National Strategy for Information Sharing and Safeguarding (NSISS) signed by the President in December 2012.

The principal achievement of the ISPB in 2012, the culmination of many months of intense preparation and effort, was the unanimous approval to share hundreds of FBI case classifications with State, Local, Tribal, and Territorial (SLTT) criminal justice organizations via N-DEx. As described elsewhere in this report, as of the end of 2012, over 70,000 total users had access to the N-DEx system. Approximately 4,000 agencies were submitting data containing over 150 million searchable records representing more than one billion entities (persons, places, things, and events). In 2012 N-DEx users gained access to 38 million records from the Department of Homeland Security and records from the Arizona Attorney General Southwest Border Anti-money Laundering Alliance. The benefit of greatly increased sharing of FBI information accrues to both SLTT authorities, and also to FBI case Agents and analysts, who now have greatly enhanced insight into SLTT investigations that intersect their own due to common interests in certain persons, places, things, and events.

Access Policy Group (APG)

The APG is a standing committee which by charter supports the ISPB and is chaired by the FBI CISO. With representatives from all FBI divisions, the APG performs assessments for and makes policy recommendations to the ISPB on user access issues, including information technology and all other aspects of user access policies; data source approvals for FBI analytic, intelligence, and investigative systems and tools; and interagency information sharing issues. It serves as the primary point of coordination for FBI information technology and operational components working on different facets of internal and interagency information sharing.

During 2012 the APG met three times. Activities covered these priorities:

- The OIC Information Access Compliance Analysis (the "Red Team");
- NCTC ingest of International Terrorism Case files from ACS, and later from Sentinel;
- Enterprise data access policy;
- Sentinel deployment and subsequent enhancements;
- Greatly increasing the amount of investigative case material that will be shared with State, local, Tribal, and Territorial criminal justice organizations via N-DEx;
- Enterprise Security Operations Center protection against insider threat;
- Issues around required reviews of manually restricted case files;

- Monitoring updates on information sharing activities in the interagency arena, especially preparing and finalizing the National Strategy for Information Sharing and Safeguarding signed by the President in December 2012; and,
- Several Government Accountability Office (GAO) reviews relevant to FBI information sharing.

Information Sharing Teams (ISTs)

ISTs are formed on an ad hoc basis in response to specific requirements from the ISPB assigned through the APG. They are chaired by subject matter experts. ISTs make policy recommendations initially to the APG for consideration and, if the APG so recommends, for subsequent consideration and approval by the ISPB. The mission of ISTs is to perform specific or targeted assessments and reviews of non-technical, information sharing policy issues relating to FBI analytic, intelligence, and investigative systems, data and tools, as directed by the ISPB and the APG. They also work in conjunction with the FBI Office of Congressional Affairs to formulate responses to Congressional requests.

Chief Information Sharing Officer

In September 2008, the EAD of the National Security Branch created the CISO position. In 2011, the CISO was named by the Deputy Director as the FBI senior official charged with overseeing classified information sharing and safeguarding, as required under the Structural Reforms E.O. 13587. In November 2012, the Chief Knowledge Officer was named as Principal FBI Executive for Knowledge Management, Information and Intelligence Sharing and Safeguarding Access Control. At that time, the CISO was reassigned to the OCKO which in turn was re-aligned to the office of the Assistant Deputy Director.

The major missions of the CISO are to coordinate FBI information sharing and safeguarding policy development to facilitate operational divisions' work; coordinate interagency policy and issues; represent the FBI at interagency forums; and to prepare strategy and annual reports, including input for the ISE Annual Report to Congress. The CISO serves as Executive Secretary of the ISPB and also chairs the APG, which carries out the direction of the ISPB.

To carry out this mission, the CISO maintains a strong liaison relationship with the Department of Justice, the National Security Staff, and the Office of the Director of National Intelligence. These entities sponsor several senior-level policy groups as well as numerous subcommittees and working groups. In addition to attending the senior-level groups, the CISO coordinates attendance and all taskings to ensure FBI equities are well represented, FBI responses are consistent, and that FBI policy and business process are consistent with the guidance and mandates that emanate from these interagency entities.

In addition to this Federal interaction, there is also coordination with the State, local, Tribal, and private sector through various working groups and committees. Finally, oversight bodies such as the GAO and Congress have a strong interest in information sharing and safeguarding, and the CISO is often called upon to participate in, serve as a key advisor for, and otherwise respond to reviews and data calls from these organizations.

In 2012, the CISO fulfilled the mandate to provide FBI representation to numerous interagency policy and information sharing organizations, including several White House National Security Staff IPCs related to information sharing and security; the Intelligence Community Information Sharing Steering Committee (IC ISSC); Department of Justice meetings related to the Law Enforcement Information Sharing Program (LEISP) and the Global Justice Criminal Intelligence Coordinating Council; and other senior groups. The

CISO facilitated, monitored, and reported on interagency information-sharing initiatives between the FBI and other organizations (including Federal, State, local, Tribal, foreign, and private partners), identifying issues and inconsistent policies, and informing policy creation and revision. The CISO also contributed to the preparation of Congressional testimony and other public statements by FBI senior leadership on information sharing topics.

CJIS Advisory Policy Board and Compact Council

The CJIS Division continues to seek the input of the nation's criminal justice community and to cooperate with that community to accomplish shared goals. The two ways in which CJIS collaborates are through the CJIS Advisory Policy Board (APB) and the National Crime Prevention and Privacy Compact Council.

The APB is chartered under the provisions of the Federal Advisory Committee Act of 1972 and consists of criminal justice professionals who provide guidance and voice the viewpoint of CJIS systems users, reflecting the efforts of one Federal and four regional working groups and numerous ad hoc subcommittees. Although the National Crime Information Center (NCIC) APB dates back to 1969, former FBI Director Louis J. Freeh expanded the advisory process to cover all CJIS services in the fall of 1994.

In 2012 the APB, consisting of 34 representatives from criminal justice and national security agencies, tackled numerous topics in the pursuit of improving and advancing CJIS systems. In its year-end meeting in December 2011, the APB recommended that the N-DEx support criminal justice employment background investigations. It was further suggested that the N-DEx Program Office incorporate into the N-DEx Policy and Operating Manual the policies and language regarding notice and consent, redress, and audits so the N-DEx system could be accessed for criminal justice employment background checks.

At that same meeting, the APB also advocated a change to the definition of rape within the Uniform Crime Reporting (UCR) Summary Reporting System. The new definition replaces the words "forcibly and against her will" with the statement "without the consent of the victim." Further, the new definition does not stipulate that the victim must be female. Consistent with the new definition, the APB also voted to remove the term "forcible" from specific sex offenses collected by the FBI's Uniform Crime Reporting (UCR) Program.

At the June 2012 meeting of the APB, the Board recommended creating a Violent Person File (VPF) in the NCIC. Statistical evidence indicates that, of offenders who feloniously kill a police officer, 44 percent have a history of violent crimes and 23 percent have a previous record for assaulting a police officer. The NCIC VPF flags individuals who meet specific criteria for inclusion based on prior convictions for assault or murder of a law enforcement officer, previous convictions for violent offenses against other persons, or past convictions for a violent offense where a firearm or weapon was used. The ability to access this information quickly through the NCIC will greatly enhance police officer safety in the field.

B. Interagency Governance

The President issued the National Strategy for Information Sharing and Safeguarding (NSISS) in December 2012 and work began on the NSISS Implementation Plan. The NSISS is the President's plan for how the Federal Government will responsibly share and safeguard information that enhances national security and protects the safety of the American people. Anchored in the 2010 National Security Strategy,

the NSISS takes a whole-of-government approach in providing guidance for more effective integration and implementation of policies, processes, standards, and technologies that promote secure and responsible national security information sharing. The NSISS Implementation Plan will be written by interagency working groups, each focused on one of the 16 priority objectives of the strategy. Priority Objective 1 is: "Align information sharing and safeguarding governance to foster better decision-making, performance, accountability, and implementation of the *Strategy's* goals." Just as the FBI supported preparation of the strategy, it will also support development of the implementation plan in the coming year (2013).

Senior Information Sharing and Safeguarding Steering Committee

This committee is co-chaired by senior executives from the Office of Management and Budget (OMB) and the National Security Staff. The FBI is regularly represented in this committee by both the Associate Executive Assistant Director of the ITB and the FBI CISO. In addition, the FBI has assigned personnel to each of the Steering Committee's elements established to carry out the Committee's policy and guidance: the Executive Agent for Safeguarding, the Insider Threat Task Force, and the Classified Information Sharing and Safeguarding Office.

Created in 2011, the Steering Committee in 2012 focused on implementing the provisions of Executive Order 13587, "Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." The five priority areas are:

1. Access control
2. Enterprise audit
3. Insider threat
4. Reduced anonymity
5. Removable media

As the year came to a close, the FBI had either fully achieved or was on track to meet or exceed all targets for the five priorities.

Information Sharing and Access Interagency Policy Committee (IPC)

The ISA IPC is the National Security Staff focal point for issues related to information sharing. Its focus extends beyond terrorism-related issues to a broad range of information sharing issues which impact national security. The ISA IPC leads an interagency policy process to identify information sharing and access priorities to more fully address the needs of Federal, State, local, Tribal, and private sector stakeholders while protecting privacy and civil liberties.

The IPC's principal focus this year was on the new NSISS and preparations for developing an associated implementation plan. The CISO represented FBI interests in the discussion on expanding the scope of the NSISS beyond that of the President's 2007 National Information Sharing Strategy, which was agreed with largely due to the broader applicability of the capabilities built specifically to support the information sharing environment. ISA IPC members were in general agreement that information related to such things as natural disasters, organized crime, and drug trafficking should be included in the definition of homeland security, and that the new strategy should take a whole-of-government approach. The CISO was similarly involved in the NSISS Implementation Plan working group.

Much of the work of the IPC occurred at the sub-committee and working group levels. The IPC has five sub-committees: Watchlisting and Screening; Fusion Centers; Suspicious Activity Reporting; Privacy, Civil Rights and Civil Liberties; and Information Integration. In each case the CISO ensured the FBI was represented appropriately, and that an FBI representative participated in each focused working group that addressed an issue touching on FBI equities.

- The Counterterrorism Division provided subject matter experts and operational expertise for the Watchlisting Subcommittee, reviewing watchlisting business processes to ensure continued improvement in information sharing among the major counterterrorism centers while safeguarding the privacy, civil rights and civil liberties of Americans;

- An FBI Deputy Assistant Director co-chaired the Fusion Center Subcommittee. In 2012 this subcommittee continued to provide executive oversight for the National Fusion Center Program Management Office on issues related to fusion center baseline capabilities;

- The Suspicious Activity Reporting Subcommittee provided executive oversight for the NSI Program Management Office and collaborated on policy with the other subcommittees; and,

- The Privacy, Civil Rights and Civil Liberties Subcommittee issued a report examining ISE Privacy Guideline revisions and, with the approval of the ISA IPC, decided to delay such a revision until after the new NSISS had been completed. The thought was that the NSISS might expand the scope and application of information sharing and safeguarding from a counterterrorism focus to include other information types.

The CISO and the ITB collaborated to ensure appropriate FBI representation on the Information Integration Subcommittee and ensured participation by highly technically qualified individuals on the associated Data Aggregation Working Group and the Identity Federation Coordination Working Group.

Office of the Program Manager for the Information Sharing Environment (PM-ISE)

During 2012 the FBI maintained a close working relationship with the Program Manager for the Information Sharing Environment (PM-ISE) and his staff, collaborating on issues arising from the ISA IPC such as the NSISS and its implementation plan, the 2011 ISE Annual Report to Congress, and the annual ISE implementation guidance. The FBI continued to engage with the PM-ISE and the NSI Program Management Office to ensure fusion centers have the necessary capabilities to receive, fuse, report, and share information appropriately with JTTTFs and other NSI partners. The DI Office of Partner Engagement (OPE) is firmly engaged on these issues.

Several other FBI offices participated in the PM-ISE interactions, depending upon the issue being addressed, especially CTD, the GMU, and the PCLU on issues relating to suspicious activity reporting. The CISO coordinated many of these interactions and also engaged with DOJ offices to ensure a fully coordinated department position was articulated in response to PM-ISE initiatives.

Intelligence Community Information Sharing Steering Committee (IC ISSC)

The CISO represented the FBI at the IC ISSC, which collaborated on information sharing issues including policy, budget, business processes, and technology. In July 2012, the NSS tasked the IC Information

Sharing Executive to assess the state of post-WikiLeaks information sharing. The major points made in a non-scientific, anecdotal report included observations that some departments and agencies are increasingly reluctant to share and an increased use of the ORCON (Originator Controlled) marking on intelligence products.

Fortunately, in spite of these observed setbacks, information sharing within the IC did not decrease overall. The use of PKI certificates across the IC to authoritatively identify system users has helped to increase confidence among intelligence producers; more secure collaborative environments were created and were being used; and there was an increase in the number of documents being posted to the Library of National Intelligence.

Significant issues remaining to be addressed include a continued need for training so that information stewards can have confidence that users are appropriately trained to properly safeguard information and share responsibly, as well as lingering uncertainty associated with moving sensitive information into a cloud environment.

The Report concludes there is a need to continue to develop a comprehensive information sharing security policy framework that addresses all networks as a unified, coherent enterprise.

C. Ensuring Accountability

The FBI's Strategy Management System includes major objectives that address providing leadership and assistance to partners, enhancing relationships, and maximizing organizational collaboration. Information sharing and safeguarding are embedded in the agency's strategy and performance management metrics.

The FBI's Senior Executives are rated on "Collaboration and Integration" as part of their performance evaluations, indicative of the Bureau's interest in rewarding information sharing efforts. In addition, each Special Agent and Intelligence Analyst has information sharing elements included in their annual performance work plans.

Based on recommendations included in the GAO report, *"Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities,"* the FBI began work through the ISA IPC to develop performance-based metrics and to identify best practices to better hold field-based information sharing entities accountable for coordination.

D. Emphasizing Awareness and Training

Numerous training courses required by the FBI for staff and contractor personnel address the secure sharing of information. Annual information assurance, handling of U.S. Persons data, handling of controlled or sensitive unclassified information, and Domestic Investigations and Operations Guide (DIOG) and other courses refresh permanent and contractor staff understanding of appropriate and secure information sharing. Elements from these courses are included in training on the use of various FBI information sharing systems such as Sentinel, enterprise email, LEO, N-DEx, eGuardian, and DIVS.

The FBI has also implemented a number of mission-specific training opportunities that support information sharing and collaboration. Newly hired Special Agents and Intelligence Analysts are taught the importance of sharing information and collaborating with external partners throughout New Agents' Training and the Intelligence Basic Course, respectively. The FBI's DI has also implemented an initiative

entitled “Dual Mission from Day One” which emphasizes the importance of collaboration and information sharing among members of the intelligence workforce within the FBI. Additionally, the FBI has developed and implemented an Onboarding New Employees course that all new hires to the FBI attend, which emphasizes the importance of collaboration and information sharing and safeguarding among members of the FBI workforce, across different job series, field offices, and work roles. The DI promotes and facilitates external training opportunities for FBI employees conducive to information sharing and collaboration throughout the IC. FBI employees participate in these sessions alongside employees from other IC agencies. The DI also collaborates with the FBI's Training Division (TD) to provide internal training requirements needed for FBI employees to perform their respective jobs related to information sharing, information safeguarding, and collaboration with partners.

The TD Outreach and Communications Unit (OCU) supports training through information sharing and collaboration in several ways. The OCU has contributed to the expansion of the Virtual Academy (VA), a learning management tool historically used to manage and promote classroom training courses, including an information sharing system that brings together additional training and learning resources across the Bureau. The VA now provides a central, online location for all FBI training information to enhance employees’ professional growth. The OCU staff edits and produces content for the FBI Law Enforcement Bulletin, now an online-only webpage after an 80-year monthly publication history. Offered online since 1989, the magazine provides readers with articles on a wide variety of law enforcement topics and has been shared with an estimated readership of over 200,000 in over 150 countries. The OCU staff has contributed to the development of improved TD intranet sites where many units now highlight special learning tools, videos, and information regarding their area of expertise (i.e., firearms training modules with videos, student sites, instructional modules).

In addition, TD's National Academy Unit (NAU) provides leadership training to executive State, local, Federal and international law enforcement and provides a networking environment that allows students and graduates to connect, share ideas and experiences, and to work together to protect their communities. The NAU supports the National Academy (NA) Associates and the National Executive Institute (NEI) Associates, allowing all NA and NEI graduates a means of staying connected with other graduates and the FBI. Information sharing and collaborative efforts among law enforcement agencies in all 50 states, the District of Colombia, and 181 different countries are facilitated for over 32,000 graduates and their departments or agencies through the NA, NEI and the Associates’ organizations. The NA Associates also coordinates with NAU to provide ongoing local, regional, and international training for NA graduates which also allows for the sharing of information and collaboration among law enforcement agencies domestically and internationally.

TD's International Training and Assistance Unit provided numerous training opportunities to the FBI's international partners. The purpose of this training is to foster relationships between the FBI's foreign law enforcement partners and to provide them with tools to modernize their law enforcement functions. In so doing, the Bureau improves information sharing and collaboration with these global partners.

In another TD effort during 2012, over 200 FBI ballistic data disks were provided to other U.S. Government and local agencies for use in selecting ammunition. Ballistic Research Facility personnel personally assisted other U.S. and select foreign government agencies in excess of 300 times in 2012.

The FBI's CTD continues to support information sharing and collaboration through the Joint Terrorism Orientation and Operations Course (JTOOC). The JTOOC is a two-week, interactive course that is used to familiarize TFOs with day-to-day investigative operations, laws, and investigative techniques for CT investigations. Approximately 260 students successfully completed JTOOC training by attending one of the seven courses offered during 2012. In addition, the Counterterrorism Investigative Operations course continues to use internal and external FBI subject matter experts to train Agents on laws, policies and competencies specific to the CT career path. It also provides enhanced instruction on investigative tools and techniques necessary for conducting successful CT investigations.

The FBI requires all employees to complete annual training regarding information sharing and safeguarding, which includes a segment on privacy. Success is measured by employees completing mandated training and being held accountable for all aspects of content in the performance of their duties. For example, all FBI National Security Branch employees are required to complete the computer-based training module: ISE Core Awareness Training within 60 days of their arrival.

E. Recognizing Success

In 2012 four individuals were recognized with Information Sharing Awards as part of a Bureau-wide recognition and best practices sharing program for employees to share proven solutions, knowledge, and experiences. These recognition awards were created to enhance awareness of information sharing goals and the central role they play in the FBI's National Security, Intelligence, and Law Enforcement missions.

VII. Way Forward

The great truth that has guided the FBI since its inception in 1908, the conviction that cooperation among law enforcement agencies and with all the people of America is key to keeping our country secure, has been demonstrated repeatedly over these many decades. It is our hope that this Report conveys the FBI information sharing efforts and accomplishments for 2012, and that it demonstrates that whatever success we may have achieved is borne of the spirit of cooperation that binds the FBI to the nation it serves. Moving forward, the FBI leadership is committed to continuing to balance the responsibility to share information with the need to safeguard the sensitive sources and methods that yielded that information, and to protecting privacy and civil liberties to fully meet our mission of ensuring the security of this nation and its people.

Appendix A: Authorities and Governing Principles for FBI Information Sharing, Privacy and Civil Liberties (Annotated) Framework

Privacy and civil liberties are deeply respected and vigorously protected by the FBI. Rigorous obedience to the U.S. Constitution, respect for the dignity of all those we protect, compassion, fairness, and uncompromising personal and institutional integrity are core values of the organization and are reflected in the implementation of FBI programs.

The vital role of information sharing in the protection of our national security has been recognized and embraced at all levels of the Federal Government. Legislation and regulations have been enacted and programs and strategies established which operationalize and mandate the principles of information sharing, all while protecting the privacy and civil liberties of U.S. Persons. The important legislation, directives, regulations and programs which mandate and authorize information sharing activities and protection of privacy and civil liberties are described below:

The U.S. Constitution and, in particular, the Bill of Rights. Especially important are the First Amendment, which protects the rights of free speech, assembly, the press and religion; and the Fourth Amendment, which prohibits unreasonable searches and seizures, and establishes the probable cause requirement for warrants.

The Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579 (Dec. 31, 1974), which governs the collection, use, maintenance and dissemination by Federal agencies of information concerning U.S. citizens and aliens lawfully admitted for permanent residence. The Act restricts what agencies can do with personally identifiable information (PII) in the absence of consent from the individual to whom the information pertains and imposes rules on agencies to be transparent about what information they collect and why.

FBI records are largely exempt from the access and amendment provisions of the Privacy Act, but as a matter of discretion, the FBI may permit one-page statements of disagreement with facts found in records to be submitted by the record holder. This process is described in 28 C.F.R. 16.46(d).

The Freedom of Information Act (FOIA), 5 U.S.C. § 552, Public Law 89-554, 80 Stat. 383 (September 6, 1966; Amended 1996, 2002, 2007); which promotes transparency of government operations by allowing any individual to request government records and to receive them, subject to applicable statutory exemptions.

Since FBI records are largely exempt from the access and amendment provisions of the Privacy Act, most individuals obtain access to FBI information through the FOIA.

Section 208 of the E-Government Act of 2002, Public Law 107–347347, 44 U.S.C. §§ 3601-3606 (December 17, 2002), as amended, which requires agencies to consider the privacy implications of their information technology systems that involve the collection and maintenance of information in identifiable form. This provision also requires agencies to prepare Privacy Impact Assessments (PIAs), which explain any privacy risks and steps taken to mitigate these risks.

As a matter of DOJ policy, the FBI conducts PIAs on all IT systems, despite the fact that national security systems are exempt from this requirement and a significant number of our systems qualify as national security systems.

Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, 6 U.S.C. § 485, Public Law 108-458 (December 17, 2004), applied the lessons of the September 11, 2001 attacks to reform the IC and the intelligence and intelligence-related activities of the U.S. Government. Among other things, the Act established the National Counterterrorism Center (NCTC), the Privacy and Civil Liberties Oversight Board, the position of Director of National Intelligence (DNI), and required the President to establish an Information Sharing Environment (ISE).

In 2007, Section 1016 of IRTPA was amended to include homeland security information as part of the ISE and weapons of mass destruction information within the definition of *terrorism*. It codifies many of the recommendations developed in response to the President's information sharing guidelines, such as the creation of the Interagency Threat Assessment Coordination Group (ITACG), and the development of a national network of State and major urban area fusion centers.

The ISE is defined in the Act as "an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section." Its principal goal is to enable and encourage the sharing of terrorism information in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties. In practice, the ISE leverages existing capabilities by adjusting and integrating current policies, business processes, standards, and systems in order to improve information sharing among all ISE participants. The authors of IRTPA carefully avoided calling the ISE a "system" or "information sharing network." The term "environment" was used to describe a virtual infrastructure or framework which enhances and streamlines information sharing in the IC.

The IRTPA also required that the ISE incorporate protections for individuals' privacy and civil liberties. The Program Manager, ISE (PM-ISE), developed guidelines in 2006, the *Guidelines to Ensure that the Information Privacy and other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment,"* and in 2010, DOJ issued its implementation guidelines, the "*DOJ Privacy, Civil Rights and Civil Liberties Protections Policy for the Information Sharing Environment*." The FBI adheres to IRTPA and to these implementation policies through its internal policies that protect privacy in the ISE.

Privacy and Civil Liberties Oversight Board, established pursuant to 42 U.S.C § 2000ee, is charged with "analyz[ing] and review[ing]" executive branch actions taken in the fight against terrorism, in order to ensure that appropriate consideration is given to the protection of privacy and civil liberties. The Board also reviews proposed legislation, regulations, and policies in order to maintain a proper balance for privacy and civil liberties. The Board also receives reports from agency privacy and civil liberties officers, and reports to Congress on its own activities.

Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801 Et Seq., Public Law 95-511, 92 Stat. 1783 (October 25, 1978), as amended, which, among other provisions, establishes a separate court to oversee the collection of foreign intelligence information via electronic surveillance and provides specific protections for U.S. Persons' information.

Executive Order 12333, United States Intelligence Activities (December 4, 1981), as amended, which governs intelligence collection activities and which states that "[t]he United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law." This Executive Order sets out the responsibilities for all members of the Intelligence Community, including the FBI.

Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans (October 25, 2005), superseded Executive Order 13356, which encouraged the sharing of terrorism information but only in a way that protects the freedom and informational privacy rights of Americans. Executive Order 13388 requires agencies to give the highest priority to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America; and to share terrorism information with all Federal, State, local, Tribal and private partners, but to do so in a way that protects the freedom, informational privacy, and other legal rights of Americans.

National Strategy for Information Sharing and Safeguarding (NSISS) (December, 2012) was issued by the White House with the goal of improving information sharing among Federal, State, and local agencies as well as private sector entities in order to improve homeland security, and also to ensure proper protection of sensitive and private information. The NSISS recognizes that there are a diverse array of threats to national security, and calls for clarifying policies relating to information sharing and correlating information across agencies as a means of combating these threats. It further notes the importance of maintaining strong protection for privacy and civil liberties, and advocates building protections for them directly into information sharing policies.

Attorney General Guidelines for Domestic Operations (AGG-DOM) recognizes the importance of conducting all activities in "a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people." These Guidelines are issued under the authority of the Attorney General as provided in Sections 509, 510, 533, and 534 of Title 28, U.S. Code, and Executive Order 12333. They apply to domestic investigative activities of the FBI and are enforced through FBI and DOJ oversight.

FBI Policy for Protecting Privacy in the Information Sharing Environment, which states that the FBI will share terrorism information (as defined in section 1016 of the IRTPA) in a manner consistent with applicable statutes, Executive Orders, Agency policies and directives, the lawful authority of the requester, and in a manner that protects the privacy, civil liberties, and other legal rights of U.S. Persons.

Domestic Investigations and Operations Guide (DIOG, October 15, 2011), which expands upon the AGG-DOM, weaves respect for privacy and civil liberties throughout the manual, making it an integral part of every investigative activity. The DIOG establishes the FBI's internal rules and procedures to implement the AGG-DOM and is enforced through internal FBI oversight, as well as review by DOJ. For example, the FBI Office of Integrity and Compliance (OIC) develops, implements, and oversees a program to ensure strict compliance with all applicable laws, regulations, rules and policies. Program managers in OIC must proactively identify legal risks and implement plans to mitigate them.

Strong oversight of the FBI by the Department of Justice, the Executive Branch, Congress and the courts:

- Intelligence Oversight Board (IOB). Reports violations of statutes, executive orders, presidential directives, regulations and other significant or highly sensitive matters to the President
- Department of Justice National Security Division (NSD). Conducts National Security Reviews for compliance with AG Guidelines and Minimization Reviews for compliance with minimization procedures
- Department of Justice Office of the Inspector General (OIG). Conducts internal investigations of suspected violations of law and internal regulations
- FISA Court. Approves minimization procedures adopted by the Attorney General
- Legislative Oversight. Senate and House Select Committees on Intelligence; Senate and House Judiciary Committees
- The Privacy and Civil Liberties Oversight Board (see above) also has the authority to review agency actions to ensure proper consideration is given to privacy and civil liberties

FBI internal safeguards:

- The OGC's Privacy and Civil Liberties Unit (PCLU), which is under the leadership of the FBI's Chief Privacy Officer. This unit reviews plans for any proposed FBI record system for compliance with the Privacy Act and related privacy protection requirements ("Privacy Impact Statements") and policies, and provides legal advice on civil liberties questions
- The criminal and national security undercover operations review committees, comprising senior DOJ and FBI officials, which review all proposed undercover operations that involve sensitive circumstances
- The Sensitive Operations Review Committee (SORC), comprising senior DOJ and FBI officials, which provides oversight of those investigative activities that may impact civil liberties and privacy and that are not otherwise subject to high level FBI and DOJ review
- The FBI requirement that all FBI employees report departures from and non-compliance with the Domestic Investigations and Operations Guide (DIOG) to their supervisors and OIC
- Training new FBI employees on privacy and periodic training for all FBI employees to maintain currency on the latest guidelines, changes to laws and regulations, and judicial decisions related to constitutional rights and liberties

Intelligence Community Directive (ICD) 501, "Discovery and Dissemination or Retrieval of Information within the Intelligence Community," was issued by the DNI and became effective on January 21, 2009. This directive charges each agency in the IC with a "responsibility to provide" information, thereby ensuring agencies can "discover" and "request" intelligence from each other in order to fulfill their respective missions. ICD 501 does not apply to purely law enforcement information. If, however, law enforcement information contains intelligence-related information, that information is subject to the Directive. In order to facilitate the efficient sharing of this information, members of the IC, including the FBI, must make all intelligence and analysis available to each other by automated means. Although there remain ways to withhold information in limited circumstances, authorized IC members who request intelligence will be presumed to have a need to know. To withhold information, an IC element must show that sharing will jeopardize the protection of sources, methods or activities, compromise a criminal or

national security investigation, or be inconsistent with the law. The ODNI has defined standards and information technology architecture requirements that all IC elements must follow to perform this process. The IC Information Sharing Executive will develop, in consultation with IC elements, including the FBI, integrated implementation plans that set forth the required benchmarks each IC element must meet in order to achieve ICD 501 policy objectives.

Law Enforcement Information Sharing Program (LEISP). The DOJ established the LEISP to achieve the Department's vision of creating relationships and methods for routinely and securely sharing criminal information across jurisdictional boundaries. It mandates the kind of wide-ranging information sharing program necessary to deter terrorism and to increase the amount of information available for the investigation and prosecution of criminal activity. The LEISP was designed in response to IRTPA requirements and Attorney General mandates for sharing DOJ data with the ISE.

The LEISP requires all DOJ components to share law enforcement information—unclassified and classified—with all law enforcement partners, with the exception of certain categories of information designated by the Deputy Attorney General (DAG). It minimizes barriers to information sharing, provides a single point of contact for DOJ information, and provides a foundation for information sharing among law enforcement at the Federal, State, local, and Tribal levels.

To advance and support the LEISP strategy, the DAG directed the FBI and other DOJ components to participate in regional and national law enforcement information sharing initiatives.[1] Accordingly, the FBI has implemented information sharing technologies which support this directive and which operationalize the FBI's National Information Sharing Strategy.

The Law Enforcement National Data Exchange (N-DEx) program is a national information sharing system designed for use by all Federal, State, local, and Tribal law enforcement agencies. N-DEx allows agencies to search and analyze data using powerful automated capabilities.

FBI National Information Sharing Strategy (NISS). The NISS is the FBI's strategy for information sharing. It provides the common vision, goals, and framework to guide FBI information sharing initiatives. The NISS complies with both the Attorney General and DNI guidelines for information sharing and seeks to balance the "responsibility to provide" with the need to protect sources, investigative operations, national security information, and the civil liberties of U.S. Persons.

The NISS has two primary objectives: to create and sustain a culture of information sharing and to develop and maintain an IT infrastructure that enables a broad spectrum of standards-based information sharing activities. The NISS identifies specific customer sets for these information sharing activities: internal FBI; Executive Branch; Federal departments and agencies; State, local, and Tribal entities; private sector; and foreign partners.

[1] See Document Library: Deputy Attorney General, Paul J. McNulty, Memorandum, "Law Enforcement Information Sharing Policy Statement and Directives," 21 December 2006.

Appendix B: Acronyms

ABAC	Attribute-Based Access Control
ABIS	Automated Biometric Identification System
ACS	Automated Case Support System
AGG-DOM	Attorney General Guidelines for Domestic Operations
APB	Advisory Policy Board
APG	Access Policy Group
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BCOE	Biometric Center of Excellence
BOP	Bureau of Prisons
CGII	California Gang Intelligence Initiative
CITWG	Counterintelligence Threat Working Group
CISO	Chief Information Sharing Officer
CJIS	Criminal Justice Information Services
CKO	Chief Knowledge Officer
CJIS	Criminal Justice Information Services Division
CORE	Collection Operations and Requirements Environment
COTS	Commercial Off-the-Shelf
CTD	Counterterrorism Division
CTF	Cyber Task Force
CTD	Counterterrorism Division
DAG	Deputy Attorney General
DEA	Drug Enforcement Agency
DEAG	Data Exploitation and Aggregation Working Group
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DIOG	Domestic Investigations and Operations Guide
DIVS	Data Integration and Visualization System
DNI	Director of National Intelligence
DOC	Department of Correction
DoD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
DSAC	Domestic Security Alliance Council
EAD	Executive Assistant Director
EDAP	Enterprise Data Access Policy
EDS	Enterprise Directory Service
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FIDS	FBI Intelligence Information Report Dissemination System
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act
FO	Field Office

FOIA	Freedom of Information Act
FTTTF	Foreign Terrorism Tracking Task Force
GAO	Government Accountability Office
GMU	Guardian Management Unit
HIDTA	High Intensity Drug Trafficking Area
HIG	High Value Detainee Interrogation Group
HSPD-6	Homeland Security Presidential Directive-6
IA	Intelligence Analyst
IAFIS	Integrated Automated Fingerprint Identification System
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
ICD	Intelligence Community Directive
IC ISSC	Intelligence Community Information Sharing Steering Committee
iDATA	Intelligence Data Association and Tagging Application
IDENT	Automated Biometric Identification System
IIR	Intelligence Information Report
IOB	Intelligence Oversight Board
IOD	International Operations Division
IPC	Interagency Policy Committee
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISE	Information Sharing Environment
ISPB	Information Sharing Policy Board
IST	Information Sharing Team
ITACG	Interagency Threat Assessment Coordination Group
JTOOC	Joint Terrorism Orientations and Operations Course
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communication System
KST	Known and Suspected Terrorists
LD	Laboratory Division
LEGAT	Legal Attaché
LEISP	Law Enforcement Information Sharing Program
LEO	Law Enforcement Online
LEO-EP	LEO Enterprise Portal
MOU	Memorandum of Understanding
N-DEx	Law Enforcement National Data Exchange
NA	National Academy
NAU	National Academy Unit
NCIWG	National Counterintelligence Working Group
NCTC	National Counterterrorism Center
NCFTA	National Cyber Forensics and Training Alliance
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NEI	National Executive Institute Associates

NGC	Next Generation Cyber
NGI	Next Generation Identification
NGIC	National Gang Intelligence Center
NGSCION	Next Generation Sensitive Compartmented Information Operational Network
NISS	National Information Sharing Strategy
NJTTF	National Joint Terrorism Task Force
NSBAC	National Security Business Alliance Council
NSD	National Security Division
NSHEAB	National Security Higher Education Advisory Board
NSI	Nationwide Suspicious Activity Reporting Initiative
NSISS	National Strategy for Information Sharing and Safeguarding
NYO	New York Office
OCKO	Office of the Chief Knowledge Officer
OCU	Outreach and Communications Unit
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPE	Office of Partner Engagement
ORCON	Originator Controlled
ORION	Operational Response and Investigative Online Network
OSAC	Overseas Security Alliance Council
PCLO	Privacy and Civil Liberties Officer
PCLU	Privacy and Civil Liberties Unit
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public-Key Infrastructure
PM-ISE	Program Manager - Information Sharing Environment
R-DNA	Rapid Deoxyribonucleic Acid
RIG	Regional Intelligence Group
SAG	Strategic Alliance Group
SAR	Suspicious Activity Reporting
SCION	Sensitive Compartmented Information Operational Network
SIG	Special Interest Group
SIPRnet	Secret Internet Protocol Router Network
SLPO	State and Local Program Office
SLTP	State, Local and Tribal, and Private Sector
SLTT	State, Local, Tribal, and Territorial
SSA	Supervisory Special Agent
STTF	Safe Trails Task Force
SWAT	Special Weapons and Tactics
TD	Training Division
TFO	Task Force Officer
TLO	Terrorism Liaison Officer
TSC	Terrorist Screening Center

TS	Top Secret
TSDB	Terrorist Screening Database
TXDPS	Texas Department of Public Safety
UCR	Uniform Crime Reporting
USIC	U.S. Intelligence Community
USMS	United States Marshals Service
USONG	United States Oil and Natural Gas
VA	Virtual Academy
VCC	Virtual Command Center
VO	Virtual Office
VPF	Violent Person File
VTC	Video Teleconferencing