Security

Since its inception in December 2001, the Security Division has developed its programs and capabilities to protect and keep Bureau personnel, information, operations, and facilities secure by providing services that enable the FBI to achieve its mission. Below are a few of the changes and accomplishments achieved by the Security Division since 2001 that support the FBI's efforts to meet changing and emerging threats.

Development of a Comprehensive Security Program

- The Security Division was created in December 2001 and has grown from 13 to 27 functional units covering physical, personnel, acquisition, and information assurance security. Total staffing has increased from 624 to more than 1,200.
- A chief security officer program was created, building a more professional security workforce.
- An information systems security officer program was established, providing day-to-day management of the FBI cyber security program.
- An acquisition security program was established in May 2004 to safeguard operations through the proactive identification, assessment, and mitigation of risks associated with the procurement of critical assets and classified contracts. Acquisition security supports the management, protection, and control of classified and sensitive information entrusted to contractors and consultants.
- An FBI security policy manual was completed December 2005; it is currently being revalidated and converted into corporate policy directives.
- The Security Division has resolved 26 of the 29 recommendations by the Webster Commission. Initiatives addressing the remaining three multi-year recommendations are in progress.

Personnel Security

- A personnel security polygraph program was established in 2001 and expanded in 2002 as a permanent element of the security investigation process for FBI personnel assigned to counterintelligence, counterterrorism, and security-related programs and for task force members, contractors, and other personnel who perform functions requiring access to FBI information, systems, and space.
- A post-adjudication risk management program was established in October 2002 to handle risk mitigation associated with the hiring of personnel representing elevated security concerns.
- A financial disclosure program was initiated in 2003 to collect detailed financial information about FBI personnel and their spouses and dependent children to support the detection and deterrence of financially motivated espionage and criminal behavior. The initial filing population increased from 200 FBI executives to more than 23,000 filers in 2010, which includes all FBI personnel with access to sensitive compartmented information, or SCI.
- Suitability and security clearance processing has been streamlined through the development and/or implementation of more than 10 different automated processing tools. These include the Electronic Questionnaire for Investigations (e-QIP) for candidate applications, the Civil Applicant System for electronic collection of candidate fingerprints, and the Clearance Verification System to report and search for current security clearance information about candidates.
- The Security Division has processed background investigations and security clearance adjudications to enable the hiring of 7,460 FBI special agents and 12,804 professional staff, as

well as security clearance investigations and adjudications for more than 14,000 local law enforcement and Joint Terrorism Task Force members.

Information Security

- The Enterprise Security Operations Center was created in 2003 as the central organization for information technology (IT) security operations.
- The Information Assurance Technology Unit was established in 2003 to develop and evaluate security technology safeguards for the FBI's IT enterprise.
- The public key infrastructure (PKI) program was established in 2005 to enable FBI IT systems and applications to increase the protection afforded to FBI information; smart card readers have been deployed to more than 30,000 FBI computer users.
- The Information Security (INFOSEC) program was initiated in 2006 to ensure the completion of mandatory annual training on the safeguards, policies, and procedures for protecting the FBI's information and IT systems.
- A technical insider threat program was established and an enterprise information protection initiative was advanced, working in close partnership with the Counterintelligence Division.
- In 2010, the Security Division spearheaded an initiative to add the law enforcement sensitive marking to the intelligence community classification and control markings register and manual. In coordination with other law enforcement agencies and intelligence community entities, marking and handling rules were created to ensure consistency and enhance information sharing with non-intelligence community partners.

Physical Security

- The scope, skill, and training of the FBI police has been expanded; a three-week post-Federal Law Enforcement Training Center training course was created to provide new officers with additional firearms and FBI policy and procedure training.
- FBI police officers were deployed in support of the Hurricane Katrina effort in Covington and Baton Rouge, Louisiana. More than 100 trips were made by 86 FBI police officers, who contributed 19,656 man-hours to the effort in 10 months.
- FBI police officers were also deployed to Puerto Rico in 2010 to participate in the largest mobilization in the FBI's history for a single-day arrest operation. The officers provided security for the operation, which resulted in the arrests of 133 suspects on public corruption charges.
- Continuity of Operations (COOP) plans were implemented and COOP coordinators were established in every FBI division; the level of participation in national-level continuity of government exercises was also increased.