Office of Security

Annual Report 2006

Homeland Security

Vision

The DHS Office of Security will create a Department in which all employees are conscious of their security responsibilities and confident in their ability to safeguard the information and resources with which they are entrusted.

Mission

The DHS Office of Security will lead a collaborative security program to safeguard the Department's personnel, information, and property so that the Department can secure the Homeland.

TABLE OF CONTENTS

Chief Security Officer's Message

The Office of Security's mission is to secure the Department so the Department can secure the Homeland. To that end, we are leading a department-wide effort to safeguard personnel, information, and property.

Today's complex security environment demands that all the Department's security professionals and operations be effectively integrated to achieve our security objectives and accomplish the DHS mission. For example, in FY-06 DHS security components furthered the Secretary's goal to accelerate and streamline information sharing with state, local, tribal, and private-sector partners. Specific initiatives included: expediting background investigations and granting security clearances; conducting facility security risk assessments; providing security education and awareness training; and issuing guidance on topics ranging from installing physical security equipment to handling classified information.

Over the past year, we have combined and strengthened security operations across the Department. We recognized several departmental Centers of Security Excellence and established the Chief Security Officer (CSO) Council. This Council brings together the Department's best security professionals to determine the most effective course for DHS security programs and ensure a uniform and consistent policy framework. In September, the CSO Council adopted a Security Strategic Plan. This plan comprises a roadmap for all DHS security organizations, identifying where we want to go and, at an operational level, how we're going to get there. It will also be the basis for benchmarking performance.

The select highlights in this report are drawn from the multiple security programs across the Department. Successes during the past year would not have been realized without assistance and collaboration from professionals throughout DHS, other federal agencies, and our non-federal partners within the state, local, tribal and private-sector communities. We look forward to furthering those collaborative and cooperative relationships throughout 2007.

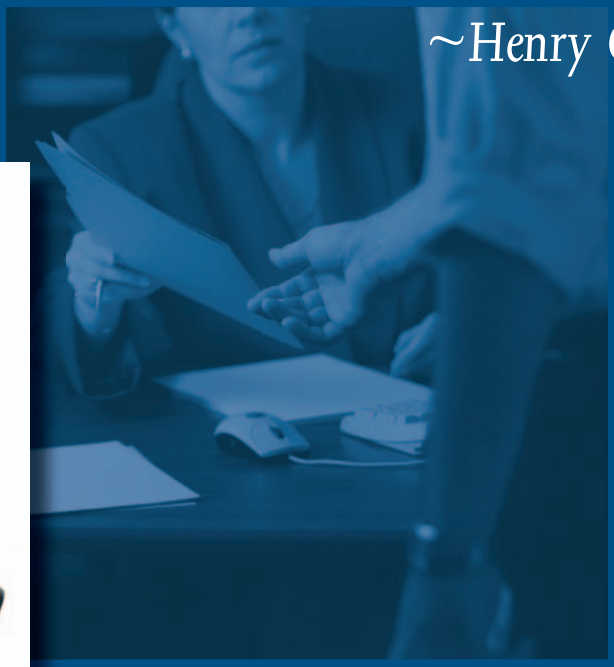
Going forward, our efforts to protect the Department's personnel, information, and property require that every security professional create an environment that rewards collaboration, promotes best practices, and shares accountability. Working together, we will provide a secure environment in which all DHS personnel can perform their Homeland Security missions.

Dwight M. Williams
Chief Security Officer
U.S. Department of Homeland Security

ENTRUSTING PERSONNEL

"Government is a trust, and the officers of the government are trustees; and both the trust and the trustees are created for the benefit of the people."

~Henry Clay



PERSONNEL SECURITY

The Office of Security ensures the highest levels of confidence in DHS employee and contractor trustworthiness, loyalty, integrity, and reliability. The Office conducts background investigations, makes suitability and security clearance eligibility determinations, and provides oversight of personnel security policy throughout the Department.

In FY-06, the Office of Security further standardized and streamlined the personnel security process. These measures included: establishing department-wide training to ensure consistency in security clearance adjudications; working to align personnel security processes with Homeland Security Presidential Directive-12 credentialing requirements; placing personnel at other federal agencies to expedite investigations; achieving DHS-wide participation in the use of the Electronic Questionnaires for Investigations Processing (e-QIP) and the Clearance Verification System; and establishing a new Personnel Security System accessible to all DHS personnel security professionals. Through these efforts the Office has significantly reduced the amount of time it takes to complete background investigations without compromising quality and comprehensiveness.

In addition to investigations and adjudications, the Office of Security continued to provide other essential personnel security-related services to the Department and its state, local, tribal, and private-sector partners in FY-06. For example, to further the Department's information-sharing mission, it adjudicated nearly 700 security clearances for state, local, and private-sector personnel. The Office also helped the Federal Emergency Management Agency (FEMA) screen the personnel who provided surge support to Hurricane Katrina recovery efforts. This enabled FEMA to meet its operational requirements. The Office launched a new fingerprinting system that enabled DHS to receive the results of fingerprint checks in as little as 24 hours. In support of DHS participation in Joint Terrorism Taskforces, the National Counterterrorism Center, and the Office of the Director of National Intelligence, the Office facilitated counterintelligence polygraphs for DHS personnel.

Finally, the Office of Security continued to be a one-stop security information source for DHS employees, responding to more than 26,000 requests and questions. The Office also issued nearly 1,000 DHS credentials, Intelligence Community badges, and courier cards; processed visit requests between DHS and other departments; and verified the security clearances of DHS personnel participating in classified meetings.

TRAINING & OPERATIONS SECURITY

The Office of Security creates a culture of security throughout the Department, ensuring that the DHS workforce is trained to recognize and defend against threats to the Department's personnel, information, and property.

In FY-06, the Office of Security expanded both its training and awareness programs. Using a variety of methods, including classroom and computer-based sessions, it delivered high-quality security-related education to thousands of DHS employees and partners. The training provided this year covered a broad range of security topics, from basic security orientation and refresher briefings to specialized instruction on the vulnerabilities of personal electronic devices. The Office placed the majority of this training, as well as links to additional resources, online to enable faster and broader dissemination.

The Office of Security also specifically designed training to meet the unique security requirements of DHS components and state and local officials. For example, it established regional OPSEC Training Centers at Federal Law Enforcement Training Center locations, training federal, state, and local government employees on how to prevent the inadvertent compromise of sensitive DHS activities and capabilities. In addition to these programs, the Office reviewed hundreds of pages of potentially sensitive information prior to release and developed nearly 40 publications addressing issues such as identity theft, foreign travel safety, and the security clearance process. Nearly 90,000 hard copies and countless electronic copies of these training materials were distributed to DHS personnel and state, local, and private-sector partners.

The highlight of the FY-06 security training and awareness program was the Third Annual Security Conference, held in Baltimore Maryland. In addition to DHS personnel, the Department's state, local, and private-sector partners participated in the Conference. More than 1,000 security management professionals from across the country took advantage of a dedicated track designed to increase their knowledge of the federal security process. By ensuring that state, local, and private-sector personnel received training on security requirements, the Office of Security furthered the Department's information sharing mission.

SAFEGUARDING INFORMATION

"Never underestimate the time, expense, and effort an opponent will expend to break a code."
~Robert Morris

ADMINISTRATIVE SECURITY

The Office of Security establishes policies, programs, and standards necessary to safeguard classified and sensitive but unclassified information.

The DHS information sharing initiative continued to evolve in FY-06 as the Department expanded its partnerships with State and Local Fusion Centers across the country. To meet these increased requirements, the Office enhanced its nationwide program to ensure the integrity and security of the classified and sensitive information shared with its state, local, tribal, and private-sector partners. Elements of this program included conducting site surveys; verifying and documenting the security environment at facilities; providing security education and training; and issuing policy guidance to provide a uniform and consistent framework. During the past year, the Office also conducted security assistance visits to intelligence and counterterrorism divisions of state and local law enforcement entities.

In FY-06, the Office of Security strengthened classification management throughout the Department. In addition to publishing several management directives and delegations of authority related to the safeguarding and handling of classified information, the Office worked with subject matter experts and program officials from the components to develop and publish specific classification and declassification guides for more than 20 programs. The Office also issued a department-wide Declassification Plan and reviewed more than 4,000 pages of documents submitted for mandatory declassification review.

The Office of Security processes and validates contractors, contract companies, and facilities pursuant to the National Industrial Security Program (NISP). In support of this program, the Office reviewed more than 200 contract statements of work; expanded its DHS-wide NISP education and outreach efforts by providing training to more than 300 contract professionals; and created a database to track classified contracts across the Department.

The Office developed the policies, standard operating procedures, and training curriculum necessary to implement a comprehensive departmental security compliance program. The Office also helped shape national-level policy in FY-06, representing the Department on multiple inter-agency committees such as the Records Access and Information Security Policy Coordinating Committee and the National Declassification Initiative Steering Committee. Similarly, it advocated for DHS on the various Information Sharing Environment working groups.

INTERNAL SECURITY & INVESTIGATIONS

The Office of Security protects DHS personnel, information and property from foreign intelligence services, terrorists, and criminals. The Office identifies, analyzes, and defends against espionage directed at DHS and conducts investigations of crimes committed against government personnel, property, and facilities.

During FY-06, DHS international agreements and information sharing initiatives continued to expand. To protect against the loss of sensitive and proprietary information the Office of Security initiated several pro-active information protection measures. For example, to address issues associated with the acquisitions and procurement process, the Office took the lead in developing an Acquisitions Security Program. When companies compete for work on DHS contracts, the Office assesses potential vulnerabilities associated with acquisition and provides a risk assessment.

As in previous years, the Department received numerous foreign visitors at its facilities. In FY-06, the Office of Security continued its efforts to detect and prevent foreign intelligence services from exploiting these visits to DHS facilities and personnel. It expanded the Foreign Access Management System and deployed the system to several DHS components. This system provides a mechanism to vet foreign visitors before they are given access to a DHS facility. To mitigate the threat posed by both foreign visits and overseas travel by DHS personnel, the Office provided a variety of counterintelligence awareness briefings to employees and contractors to help them recognize foreign intelligence activities, deflect elicitation attempts, and avoid becoming unwitting enablers of a foreign intelligence service.

During FY-06, the Office of Security expanded and enhanced its working relationship with the Federal Bureau of Investigation (FBI) on counterintelligence-related and espionage initiatives with a nexus to DHS. This interagency collaboration continues to ensure that investigative referrals are made to the FBI in a timely manner, while maintaining the Secretary's ability to protect the Department from foreign intelligence collection activities.

In addition to its counterintelligence-related mission, the Office of Security conducts investigations on behalf of components without an investigative capability and, when appropriate, in coordination with the Office of the Inspector General. In FY-06, the Office's investigative caseload increased. The Office investigated several crimes committed on DHS property or against persons on DHS property, including theft from headquarters facilities, abuse of official credentials, and misuse of government computers. It also referred these investigations to the appropriate authorities for prosecution or administrative action. Finally, the Office reviewed numerous background investigations to assess whether incidents affected an employee's ability to hold a security clearance.

SPECIAL SECURITY PROGRAMS

The Office of Security manages the DHS Sensitive Compartmented Information (SCI) and Special Access Programs.

In FY-06, the Office published a comprehensive SCI Administrative Handbook that provides information on self inspection and compliance-related tools for SCI program managers. It also supported DHS SCI program managers by conducting on-site assistance visits to component SCI Facilities (SCIF) throughout the United States.

During FY-06, the Office of Security consolidated DHS SCIF accreditation records. Accreditation certificates for DHS SCIFs issued prior to the creation of DHS were formally transferred from the original accrediting authority to the Office of Security. The Office then visited these facilities to verify and recertify their accreditations. Based upon these reviews various corrective actions were initiated to ensure compliance with U.S. Intelligence Community (IC) standards and DHS Management Directives. In addition to reaccrediting existing SCIFs, the Office of Security accredited several new SCIFs.

To assist DHS SCI-cleared personnel the Office of Security created, published, and disseminated a standard annual SCI refresher briefing. It presented this briefing to more than 1,500 personnel at DHS headquarters, Federal Emergency Management Agency, Immigration and Customs Enforcement, and Citizenship and Immigration Services. Additionally, in an on-going effort to standardize training and career development requirements for DHS Special Security Officers (SSO) and Special Security Representatives, the Office coordinated department-wide training.

In support of the Director of National Intelligence (DNI) and other IC community agencies, Office of Security personnel participated with their IC colleagues on working groups to transition IC Directives and policies from the Director of Central Intelligence to the DNI.

PROTECTING PROPERTY

"Let us not look back in anger or forward in fear, but around in awareness."
~James Thurber

PHYSICAL SECURITY

The Office of Security protects DHS personnel, controls access to DHS headquarters facilities, and safeguards against damage and theft.

In FY-06, the Office conducted a comprehensive review of physical security procedures at the Nebraska Avenue Complex (NAC). This review established the baseline requirements for perimeter security enhancements as well as for a new guard force contract. Under the supervision of the Office of Security, the guard force enabled access to the complex for more than 40,000 visitors and responded to security-related incidents, including emergency and fire alarms, suspicious vehicles and packages, reported thefts, and traffic accidents.

In addition to the NAC, the Office of Security provided security design, construction, and equipment-installation services to headquarters facilities throughout the National Capital Region. These services included guidance and operational support regarding alarms and access control equipment, closed circuit television systems, intrusion detection systems, X-ray machines, magnetometers, and locking devices. Other physical security services provided in FY-06 included facility and residential surveys, pre-lease inspections, and technical sweeps of secure facilities to identify security vulnerabilities and recommend corrective measures.

The Office of Security leads the DHS-wide program for implementation of Homeland Security Presidential Directive 12 (HSPD-12), which requires a secure, interoperable, and reliable form of identification for federal employees and contractors. In FY-06, the Office met all HSPD-12 requirements by deploying a compliant credentialing system and associated policy and procedures; developed an HSPD-12 implementation strategy plan that will be used to facilitate component rollout; and completed a Privacy Impact Assessment and published a System of Records Notice (SORN) in the Federal Register to ensure protection of system records and document privacy protection mechanisms.

In FY-06, the Office of Security continued its administration of the Interagency Security Committee (ISC), which is chaired by the Chief Security Officer. This year, the ISC issued Safe Mail Handling Best Practices for federal agencies; held its first Biennial Planning Conference to develop an Action Plan; and worked with the Governmental Accountability Office to address recommendations for enhancing security at federal facilities.

POLICY

The Office of Security develops and coordinates department-wide security-related polices to ensure consistency and integration of the Department's security mission.

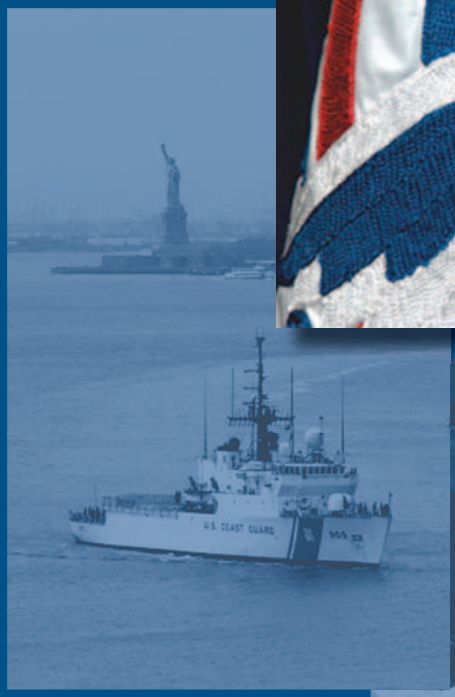
This past year, the Office issued Management Directives (MD) aligning the DHS security mission with the overall DHS mission. Specifically, MD 11000 *Office of Security* established the responsibilities of the Office and defined its mission of safeguarding the Department's personnel, information, and property. MD 11080 *Security Line of Business Integration and Management* is the principal document for governing, integrating, and managing security functions throughout DHS. To further the functional integration of component security offices, the Office of Security created the Chief Security Officer (CSO) Council to provide a forum for senior DHS security officials to work together to create world-class security programs. The Council addresses issues affecting the DHS security community and develops and implements a vision and strategic direction for security across the Department.

In addition to publishing MDs, the Office obtained delegated authority for the CSO to designate DHS employees as law enforcement officers and agents in accordance with Section 1706 of the Homeland Security Act of 2002 (codified at 40 U.S.C. § 1315). The Office also obtained delegated authority for oversight of the DHS Sensitive Compartmented Information (SCI) program from the Director of National Intelligence.

Consistent with DHS goals and objectives, Office of Security-issued MDs and delegated authorities have identified the CSO as the single point of contact for security issues affecting the Department. This allowed the CSO to undertake department-wide strategic planning leading to the issuance of the Security Strategic Plan. This plan, which was approved by the CSO Council, provides a roadmap for streamlining security policy across the Department.

Office of Security-issued MDs with Department-wide impact may be found on the DHS intranet, *DHSOnline*, under Components> Management> Security.

COMPONENTS



"By failing to prepare, you are preparing to fail."
~Benjamin Franklin

U.S. CITIZENSHIP & IMMIGRATION SERVICES

Chief Security Officer Rick S. Henson

The USCIS Office of Security and Investigations (OSI) provides physical and personnel security services for both USCIS Headquarters and field facilities. In addition OSI conducts internal USCIS investigations and integrity inquiries in coordination with the DHS Office of the Inspector General. During FY-06, OSI realigned its organizational structure into four divisions: Protective Security Operations, Personnel and Industrial Security Operations, Internal Investigations and Integrity Operations, and Threat Management Operations. OSI also stood up the USCIS Command Center, which provides valuable protective intelligence, situational awareness, and real-time common operating picture information to USCIS leadership. This structure allows OSI to deliver professional, proactive, modern, and cost effective security services to both its internal and external customers.

In FY-06, OSI identified a requirement to establish an automated case management system that would serve as an operations "hub." To address this requirement, an internal case management system named Joint Analysis Security Management and Investigation Network (JASMIN) was developed. OSI acquired the platform to operate the system and is finalizing acquisition of the required software. When complete, JASMIN will provide an end-to-end security and investigations data system that supports OSI investigations and all other operations in an integrated context and enables data evaluation and analysis.

In the aftermath of Hurricane Katrina OSI sent a Security Recovery Team to the USCIS New Orleans District Office to address security concerns including securing and removing all classified material and Alien Files. This deployment afforded OSI the opportunity to assess the USCIS Continuity of Operations Program (COOP). To enhance USCIS's ability to implement an effective COOP, OSI conducted a series of one-week training sessions for designated COOP coordinators and alternates. OSI also worked with National Capitol Region emergency response officials and developed a prototype common identification protocol, the "First Responder Authentication Credential." This credential is designed to facilitate first responder and senior personnel movement during crisis situations and to gain access to crisis locations.

In FY-06, OSI developed a program to increase security awareness throughout USCIS. In coordination with the Office of the Chief Human Capital Officer and the USCIS Academy, USCIS journeyman Adjudications Officers received briefings on OSI programs, activities, and services. The briefing provided points of contact for security and integrity-related questions, outlined OSI responsibilities, and reinforced security best practices. Additional training initiatives included presentations of the Critical Response Options Security and Survival (CROSS) Training as part of the International Security Program. This training was designed for USCIS personnel and their unique mission overseas, including specific security and protective operations procedures.

UNITED STATES COAST GUARD

Chief Security Officer John G. Steele

The Coast Guard's Office of Security Policy and Management provides policy direction for the protection of Coast Guard (CG) personnel, assets, classified material, and facilities throughout the United States and overseas. In FY-06, the Office developed and implemented several initiatives to strengthen Coast Guard security; aligned Coast Guard security priorities with field expectations and DHS-wide initiatives; and began to implement the recommendations of the Coast Guard Security Trends and Analyses Report, a comprehensive review of physical security vulnerabilities identified during the past two years.

The Coast Guard Security Center (SECCEN) serves as the central adjudicating facility for the processing and maintenance of all Coast Guard personnel security files. In FY-06, the SECCEN assumed Sensitive Compartmented Information (SCI) adjudication responsibilities for CG personnel from the Department of the Navy. As a result, it now handles adjudications for all Coast Guard military, civilian, and auxiliary personnel. In addition, the Security Center processed DHS state, local, and private-sector partners for clearances to support the Department's information sharing initiatives.

This past year, the Office of Security Policy and Management participated in an Antiterrorism/ Force Protection Working Group to formulate ways to better protect Coast Guard personnel and assets from acts of terrorism. The Working Group reviewed current policy related to threat conditions. As a result, the Coast Guard took specific threat mitigation measures and began making adjustments in its overall security posture. Going forward, these measures will provide a sustainable and realistic approach to protecting against and reacting to the terrorist threat. The Working Group also developed a methodology to better identify critical assets and provide the resources for their protection. Based on this methodology, the Coast Guard began reviewing more than 1,200 units and facilities. Developing these tailored security standards and measures will help to protect Coast Guard shore installations aviation commands, and mobile units operating both domestically and overseas.

The Office continued development of a security web site in FY-06. The site will provide Coast Guard security professionals real-time information pertaining to all security disciplines. The web site will also enable a two-way flow of information between headquarters and field security managers. Once deployed, the site will greatly improve security situational awareness within the Coast Guard.

U.S. CUSTOMS & BORDER PROTECTION

Assistant Commissioner, Office of Internal Affairs, James F. Tomsheck

The CBP Office of Internal Affairs (IA) has oversight authority for security aspects of operations, personnel, and facilities. Within IA the Security Management and Personnel Security Divisions are responsible for the physical, information, industrial, internal, operations, and personnel security programs.

In FY-06, the Divisions assessed the security needs of CBP facilities nationwide. Multiple site visits were conducted to assess facility security posture—including unique operational areas such as sea, air, and land ports of entry—to determine if the requirements and objectives of the CBP security program were being addressed. Personnel also responded to multiple security-related incidents at CBP Headquarters and established a database of CBP facilities, operational areas, and projects worldwide.

To enhance security awareness CBP Operations Security (OPSEC) personnel distributed OPSEC "badges" that described the OPSEC process and identified CBP critical information. They also conducted security awareness briefings and performed pre-publication reviews of CBP documents. In conjunction with other CBP security personnel, access control card issuance procedures were revised to increase accountability and the CBP Visitor Access Program was updated to enhance the efficiency of Visitor Center operations. In addition, CBP Information Security (INFOSEC) personnel drafted security classification guides, conducted a nationwide data call on CBP security containers, and represented CBP on multiple inter and intra-agency working groups.

In FY-06 Personnel Security Division employees streamlined applicant intake procedures and the pre-employment process. They resolved programming issues with the Electronic Questionnaires for Investigations Processing (e-QIP), standardized adjudicator training by developing an evaluation form, and established an internal web page to address frequently asked questions and provide contact information.

FEDERAL EMERGENCY MANAGEMENT AGENCY

Chief Security Officer Gregory Cooper

The FEMA Security Branch is responsible for the protection of all FEMA facilities, personnel, resources, classified and sensitive information, and disaster victim information.

In FY-06, FEMA Security supported DHS's information sharing initiatives by providing security assessment and certification services to state emergency operations centers and other facilities. In addition, FEMA Security assisted federal and state law enforcement agencies in locating hundreds of individuals who illegally applied for disaster relief funds after Hurricane Katrina.

FEMA Security supported disaster relief efforts in several additional ways. To expedite the massive disaster-worker hiring efforts, FEMA Security deployed portable electronic fingerprinting machines to disaster offices in five states and processed nearly 35,000 sets of fingerprints. FEMA Security increased the number of on-call Security Disaster Assistance Employees by nearly 40 percent to meet the increased demand stemming from hurricanes, tornadoes, floods, power outages, and other major disaster operations. In FY-06, these employees provided security oversight to FEMA disaster facilities and operations and responded to dozens of disasters. FEMA Security also implemented an Identity Theft Awareness Program for use at Joint Field Offices and National Program Service Centers to educate staff on ways to protect the personal information of disaster victims.

In FY-06, FEMA Security conducted security assessments of and managed the security forces at 23 FEMA facilities nationwide. It also conducted periodic inspections of 13 Critical Infrastructure Protection Program facilities. FEMA Security processed suitability and security clearance background investigations on FEMA personnel including 8,000 Disaster Assistance employees, 9,000 Urban Search and Rescue workers, and 9,000 National Disaster Medical System intermittent employees.

In addition to protection of facilities and personnel, FEMA Security is responsible for ensuring the proper handling of classified and sensitive information. In FY-06, FEMA Security provided Technical Surveillance Counter Measures support to all FEMA facilities that process, discuss, or store classified information and declassified 142,805 documents.

FEDERAL LAW ENFORCEMENT TRAINING CENTER

Chief Security Officer Ronald M. Edge, Jr.

The FLETC Security and Emergency Management Division (Security Division) develops and implements FLETC enterprise-wide security and emergency management programs in support of FLETC administrative, operational, and training missions worldwide. In FY-06, the Security Division enhanced FLETC's physical, information, and internal security programs, aligned them with DHS priorities, and developed plans for responding to emergencies.

This past year, the Security Division established comprehensive physical security and administrative security programs. As part of the physical security program, the Division revised and updated all FLETC Directives related to the physical security of its facilities and personnel. The Division also coordinated security surveys and assessments of all FLETC mailroom, shipping, and receiving facilities. A highlight of the administrative security program was the implementation of a formal review process to ensure sensitive but unclassified (SBU) information is identified and disseminated only to personnel with a need-to-know.

FLETC regularly receives visits from high-ranking foreign law enforcement and military officials sponsored by the U.S. Department of State and other federal agencies; guest law enforcement instructors; and students and their family members. In FY-06 the Security Division established a program to ensure foreign national visitors have been vetted prior to being granted access to FLETC facilities and personnel.

The Security Division implemented plans for handling emergency and crisis situations in FY-06. It coordinated the Continuity of Operations (COOP) plans for all FLETC facilities. The Division also worked closely with the FLETC Chief Information Officer to develop a comprehensive information technology COOP plan. These plans provide for continuing operations in the event of a major catastrophe or disaster. The Division completed comprehensive reviews of the Hurricane Response Plans for its facilities in Georgia and South Carolina; updated the plans based on lessons learned from recent events; and conducted scenario-based exercises to validate the plans and to ensure the inclusion of local emergency management personnel.

Chief Security Officer Traci A. Lembke

Within ICE security responsibilities are shared between the Office of Professional Responsibility (OPR) and the Federal Protective Service (FPS).

The ICE OPR implements a component-wide personnel security program. In FY-06, the OPR processed nearly 10,000 background investigations. Of these investigations, more than one-third determined Entry-On-Duty (EOD) eligibility while other investigations were performed to grant security clearances. OPR also provided a tracking mechanism for the background investigation process for each ICE employee through the Security Activity and Reporting System (SARS). SARS provides adjudication, clearance status, EOD, and investigation status information and has more than 33,000 active electronic records.

In FY-06 OPR also provided more than 3,600 ICE employees with national security information briefings; conducted 25 preliminary inquiries involving the improper handling of classified national security information; and provided security requirements and guidance for the nation wide deployment of the Homeland Security Data Network.

FPS's primary mission is to protect approximately 8,800 General Services Administration (GSA) owned or leased federal facilities. In FY-06, FPS conducted 2,480 physical security assessments of these facilities to evaluate risk and identify mitigating security countermeasures. FPS also procures contract guard services, oversees guard force operations, and provides training for approximately 15,000 contract security guards.

As a part of its protective mission, FPS provides a law enforcement response to criminal acts occurring on federal property. In FY-06 FPS made 6,319 arrests, responded to 1,642 disturbances on federal property, and investigated thousands of leads related to potential criminal incidents.

To support its law enforcement and security missions FPS operates four MegaCenters. These Mega Centers, which operate on a 24-hour basis, dispatch officers and provide a communications link between responding officers and contract guards.

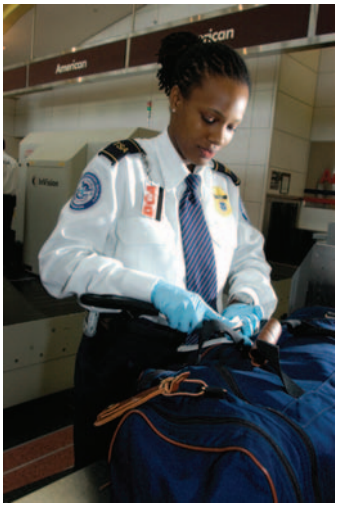
TRANSPORTATION SECURITY ADMINISTRATION

Chief Security Officer Douglas Callen

The TSA Office of Security promulgates, develops, and implements internal and personnel security policies and procedures to ensure a safe and secure work environment for all TSA employees and visitors.

During FY-06, the Office of Security became part of the TSA Office of Law Enforcement/Federal Air Marshal Service (FAMS) and continued its ambitious agenda to consolidate security programs into a centralized security office. The office assumed management of TSA's personnel security program, gained control and oversight of the TSA Sensitive Compartmented Information (SCI) Program, and took responsibility for the Annapolis Junction facility, which supports the Secure Flight program. The addition of these program responsibilities brought the office into full alignment with the DHS Office of Security.

In FY-06, to meet summer travel demands, the Office initiated a special program in conjunction with the TSA Offices of Security Operations and Human Capital to hire Transportation Security Officers (TSO). Internal personnel security processes were adjusted and resources re-allocated to facilitate the adjudication of more than 19,000 TSO applicants, making 10,000 eligible for entry on duty. This program allowed TSA to meet its operational requirements while maintaining the integrity of the personnel suitability process.



The Office also deployed the Computer Emergency Notification System (CENS) at both TSA Headquarters and the Transportation Security Operations Center (TSOC). CENS is an Office of Security controlled software program that has the capability to immediately flash emergency information on all employees' computer screens. In real time, the system communicates details of a specific emergency and provides instructions to all employees. CENS is a cost effective means to save lives, keep employees well informed, and help prevent unnecessary building evacuations and lost productivity.

In FY-06, the Office of Security continued performing site security surveys and equipment installations at Federal Security Director offices, FAMS field offices, Mission Support Centers, and other field facilities. At TSA Headquarters, the Office conducted a comprehensive review of the security guard contract and post assignments. This review resulted in a current year savings of approximately $60,000 and an out-year annual savings of more than $200,000. This review also established contingencies for a surge capability, better utilization of staff for maximum effective coverage, and provided consistent processing of employees and visitors through the Visitor Appointment Centers.

In addition to the above accomplishments, the office developed comprehensive long-range strategies to enhance physical security programs; improved Information Security (INFOSEC) procedures; disseminated security awareness and Operations Security (OPSEC) messages; expanded cooperative endeavors among law enforcement functions; and placed additional focus on personnel security issues.