



U.S. DEPARTMENT OF
ENERGY

Headquarters Security Quick Reference Book

ACRONYMS

BAO	Building Access Only	HSO	HQ Security Officer
CMPC	Classified Matter Protection and Control	LA	Limited Area
CUI	Controlled Unclassified Information	OPSEC	Operations Security
FACTS	Foreign Access Central Tracking System	OOU	Official Use Only
DOE	Department of Energy	PII	Personally Identifiable Information
E.O.	Executive Order	PIV	Personal Identity Verification
FOCI	Foreign Ownership, Control or Influence	RF	Radio Frequency
FOIA	Freedom of Information Act	SECON	Security Conditions
HSPD	Homeland Security Presidential Directive	SSIMS	Safeguards and Security Information Management System
HSS	Office of Health, Safety and Security	TSCM	Technical Surveillance Countermeasures
HQ	Headquarters	UCNI	Unclassified Controlled Nuclear Information
HQFMSP	HQ Facilities Master Security Plan		
HSIPM	HQ Security Incident Program Manager	VTR	Vault-Type Room

INTRODUCTION

This quick reference guide provides an overview of Department of Energy (DOE) Headquarters (HQ) security programs.

More detailed information can be found in the DOE *Headquarters Facilities Master Security Plan* (HQFMSP), which provides detailed instructions for the implementation of DOE safeguards and security requirements as published in a number of DOE orders, policies, notices, and guides. The HQFMSP is available at: <http://www.hss.doe.gov/hqsecop/hqfmosp/>

The complete set of security directives is available at: www.directives.doe.gov

Each HQ program and staff office participates in the HQ Security Officer (HSO) Program and designates its own HSOs. Your HSO is your primary source of information and assistance regarding security requirements and responsibilities. He or she works closely with the Office of HQ Security Operations and is familiar with the HQFMSP requirements.

Your **HSO** is _____

and can be reached at _____.

Headquarters Security Quick Reference Book

TABLE OF CONTENTS

DOE Headquarters Security Program Overview	4
Access and Personnel Security	4
Badging and Access Authorization.....	4
Visitor Access to HQ Facilities.....	7
Escort Requirements in HQ Facilities	8
Visits/Assignments by Persons Who Are Not U.S. Citizens	8
Required Processing by the HSO	8
High-Level Protocol Visits	9
Emergency Visits to the Principals	9
Physical Security.....	10
Building Access Controls	10
Hours of Operation	11
Security Areas.....	12
Prohibited Articles	12
Controlled Articles.....	13
Information Security	15

Classified Matter Protection and Control (CMPC)	15
Need-to-Know	16
Access and Use.....	17
Storage.....	18
Accountable Matter	19
Classification Review	19
Controlled Unclassified Information	20
Incidents of Security Concern.....	23
Operations Security (OPSEC).....	25
Security Awareness	25
Headquarters Security Surveys	26
Technical Surveillance Countermeasures (TSCM).....	27
Foreign Ownership, Control or Influence (FOCI)	29
Facility Clearance and Approval.....	29
HQ Equivalencies and Exemptions.....	30
HQ Security Contacts, Facility Diagrams, and Bus Schedule	31
DOE HQ Security Conditions (SECON) System	37

DOE Headquarters Security Program Overview

DOE has established a comprehensive security program for protecting personnel, information, and government property at its HQ facilities from an array of potential threats. DOE HQ security procedures are contained within the HQFMSP and are available at: <http://www.hss.doe.gov/hqsecop/hqfmisp/>. HSOs, Alternate HSOs, and HSO Representatives within each HQ element work closely with the Office of Headquarters Security Operations to ensure that DOE security requirements are implemented effectively throughout DOE HQ. HSOs perform many security functions on behalf of personnel within their elements and assist them in complying with local security procedures. Should you have questions concerning the security program or need assistance in this area, please contact your designated HSO.

Access and Personnel Security

Badging and Access Authorization

All personnel wishing to enter DOE HQ facilities to conduct official business must obtain appropriate security credentials in the form of permanent or temporary security badges. Your HSO is responsible for assisting you in submitting requests for your DOE HQ security badge, which gives you access to DOE HQ facilities and if required, a security clearance that gives you “access authorization” to classified matter and higher level security areas.







Whether or not access authorization (a security clearance) to classified matter is needed, all new DOE Federal and contractor employees are subject to personal identity verification (PIV) in compliance with Homeland

Security Presidential Directive 12 (HSPD-12). All employees are required to present two forms of identity and are subject to investigation before they can be issued a PIV approved badge. Once approved, you may obtain your security badge at the Forrestal or Germantown Badge Offices, both located on the first floors of their respective buildings. Employees whose job functions do not require access authorization are issued Building Access Only (BAO) badges. A BAO badge provides access to the building only – not Security Areas.

Access authorization must be granted in order to use, view or possess classified matter and to gain unescorted access to a Limited or greater security area. Because of the significance of the human factor in security vulnerabilities, the Office of Headquarters Personnel Security Operations' goal to protect national security is a critical element in the Department's overall security strategy. The Office of Headquarters Personnel Security Operations is committed to assuring the integrity and dependability of each individual who is granted an access authorization.

In accordance with 10 Code of Federal Regulations 707, a negative drug test result is required before an initial security clearance can be granted and personnel possessing access authorization are subject to random drug testing throughout the year.

DOE grants "Q" and "L" access authorizations depending on the type and level of information an employee needs to perform duties and responsibilities. The chart below reflects the levels and categories of classified information each allows. A "Q" requires a full field single scope background investigation (SSBI); an "L" requires national agency checks and other inquiries.

HSPD-12	LSSO (LOCAL Site Specific Only)	Access Authorization	Restricted Data (RD)	Formerly Restricted Data (FRD)	National Security Information (NSI)
 <p>FEDERAL EMPLOYEE "Q" CLEARED DOE JOHN, W Headquarters Q Emergency Response Official</p>	 <p>Badge Number US Department of Energy Washington DC LSSO First L NAME EXPIRES: MMM DD YY</p>	“Q”	Top Secret Secret Confidential	Top Secret Secret Confidential	Top Secret Secret Confidential
 <p>FEDERAL EMPLOYEE "L" CLEARED DOE JOHN, W Headquarters L</p>	 <p>Badge Number US Department of Energy Washington DC LSSO First L NAME EXPIRES: MMM DD YY</p>	“L”	--- --- Confidential	--- Secret Confidential	--- Secret Confidential
 <p>CONTRACTOR EMPLOYEE UNCLEARED DOE JOHN, W Headquarters O</p>	 <p>Badge Number US Department of Energy Washington DC LSSO First L NAME EXPIRES: MMM DD YY</p>	Uncleared	NOT AUTHORIZED FOR ACCESS TO CLASSIFIED INFORMATION		

Once you receive your security badge, you must wear it on your person above the waist at all times when in DOE facilities. For operational security reasons, you should remove your badge when you leave the building in order to reduce the potential for being targeted by hostile intelligence, terrorists, criminals or other threats.

If you lose or misplace your badge, contact the Badge Office as soon as possible and complete a Lost/Stolen Badge Report. While there can be as much as a two-week waiting period to obtain a permanent replacement HSPD-12 badge, you may obtain a temporary security badge for use until it arrives.

DOE security badges are the property of the U.S. Government and must be returned to either of the HQ Badge Offices if you are transferred, terminate employment, or otherwise no longer require a badge. Out-processing procedures for both Federal and contractor employees must be followed to ensure the return of all government property and the cancellation of access to HQ facilities and security interests. Please contact your HSO for additional guidance when out-processing.

Visitor Access to HQ Facilities

All visitors who do not have a DOE security badge, regardless of clearance status, are required to present appropriate identification and sign in at the facility's main entrance lobby. The receptionist or security personnel will verify that the visitor has been authorized by the hosting organization. If not, the hosting office will be contacted to confirm that the visitor may be admitted. Once approved, and after submitting to a security inspection at the security screening area, the visitor will be issued a visitor's badge and can enter the facility.

Escort Requirements in HQ Facilities

During normal operating hours, 6:00 a.m. to 7:00 p.m., Monday through Friday, visitors entering HQ facilities do not generally need an escort unless specified by the office or person being visited. However, visitors who will be accessing a Security Area (discussed under “Physical Security,” below) must be escorted at all times and all days. If a visitor escort is required, the sponsoring office is responsible for providing the escort. Escorts must remain with the visitor at all times and must be knowledgeable of security policy at HQ.

Consult the HQFMSP or your HSO for a copy of the HQ Escort Procedures.

Visits/Assignments by Persons Who Are Not U.S. Citizens

HQ visits and assignments by non-U.S. citizens must be approved by the Secretary, Deputy Secretary, Undersecretary, or Program Secretarial Officer or their designee prior to the visit. Visits can be up to 30 days; an assignment is 31 days or more.

Contact your HSO to arrange for a foreign visit or assignment.

Required Processing by the HSO

- Develop security plans and complete required reviews.
- Enter visit/visitor data into the Foreign Access Central Tracking System (FACTS).
- Ensure that escorts know their escorting responsibilities.
- Ensure that hosts are U.S. citizens and know their hosting responsibilities.

High-Level Protocol Visits

- These are visits to the Secretary, Deputy Secretary, Undersecretaries, or Program Secretarial Officers.
- Only visits by diplomats or senior foreign government officials are included in this category.
- A request memorandum must be submitted to the Office of Physical Protection before the visit (Room 1G-042 or fax to 6-7952).
- The visitor must be approved in FACTS *the day of* the visit.

Emergency Visits to the Principals

If you need to arrange an emergency visit to the Secretary, Deputy Secretary, Undersecretary, or Program Secretarial Officer, contact a Protective Force Officer. The Officer will notify the Office of Physical Protection at 202-586-8075. Also inform your HSO, who must ensure that the appropriate information is entered into FACTS the next business day.

After normal business hours, contact the Protective Force at:

Forrestal: 202-586-6900

Germantown: 301-903-2403

Physical Security

The mission of the Office of Physical Protection is to protect DOE facilities in the Washington, DC area; provide for the security of personnel assigned to those facilities; and ensure that classified, sensitive, and unclassified property within these facilities is properly protected.

Building Access Controls

Access to HQ facilities is controlled by a combination of automated turnstiles, badge readers, Protective Force personnel, and locked/alarmed doors. To gain entry at locations where both a badge reader and Protective Force Officers are stationed (such as the main lobbies), employees are required to hold their permanent DOE security badge near the reader on the automated access control system. Once authorized entry by the automated system, individuals must show their badges to the Protective Force Officer who will make sure the badge photo matches the individual displaying the badge. To gain entry at an automated turnstile, employees are required to hold their permanent DOE security badge near a reader on the automated access control system and enter their four-digit Personal Identification Number (PIN). If you accidentally exit an alarmed door, remain at that location until a Protective Force Officer arrives on scene and secures the door.

On entering or exiting the building:

- DOE Federal and contractor employees and their hand carried articles may be randomly inspected.
- All employees or contractors who have temporary badges are inspected upon entry and may be inspected upon exit.

At both the Forrestal and Germantown facilities, all vehicles must enter the property through security gates staffed by DOE Protective Force Officers. Federal and contractor employees must show their DOE security badge to the Officer to gain entry to the facility. All vehicles are subject to random vehicle inspection when entering the property.

All visitors arriving by vehicle onto DOE property must present some sort of government-issued photo identification for inspection by the Protective Force Officer. Drivers are required to present a valid driver's license. Visitors who intend to enter the facilities will be directed to visitor parking for visitor registration and badging. Visitors who do not intend to enter the building (e.g., vendor delivery) will be issued badges that expire on the date of issue.

Protective Force Officers inspect all visitors' vehicles prior to entry. Employees who are hosting visitors should advise them before the date of the visit that they are required to have identification documents and that their vehicle will be inspected. Hosts should also advise visitors to plan for the additional time it will take them to be processed onto the property.

All drivers should be extremely attentive when entering DOE property to ensure that the Active Vehicle Barrier is completely lowered before driving through.

Hours of Operation

Normal operating hours are 6:00 a.m. to 7:00 p.m., Monday through Friday.

Times other than normal operating hours are called *security hours*. During security hours, all DOE Federal and contractor employees and visitors will be inspected upon entry and are subject to inspection upon departure from HQ facilities. Individuals who do not consent to an entrance inspection may be denied access.

Security hours are 7:00 p.m. until 6:00 a.m. Monday through Friday, and all hours on Saturdays, Sundays, and holidays.

Security Areas

Limited Areas (LAs) and Vault-Type Rooms (VTRs) are Security Areas established specifically to protect classified matter and activities. At HQ, these areas have clearly defined boundaries and access control points. Access to these Security Areas is limited to appropriately cleared and authorized individuals. If an uncleared individual requires access to a Security Area, that individual must be escorted by a cleared individual knowledgeable of his/her escort responsibilities.

Prohibited Articles

Prohibited articles are not allowed into DOE HQ facilities, and signs identifying prohibited articles are posted at DOE facility entrances. Prohibited articles include:

- Weapons
- Explosives
- Alcoholic Beverages
- Controlled Substances (e.g., illegal drugs and/or paraphernalia) – *prescription medicines are not prohibited.*

Controlled Articles

As defined by DOE orders, controlled articles are devices (usually electronic) that can record or transmit images, conversation, or data and are therefore not routinely allowed into areas where classified material is normally present. DOE orders identify the following as controlled articles:

- Cameras
- Laptop computers, netbooks, iPads, and similar computerized devices
- Cellular phones
- Blackberries and similar devices, such as Smartphones
- Personal digital assistants
- eBook readers
- Recording devices
- Wireless devices that can store data via fixed or removable media, such as some electronic picture frames
- iPod and MP3 type devices
- Electronic toys.

DOE HQ Exception: Under certain conditions, DOE policy allows specifically designated controlled articles into LAs that are authorized for storing, processing, and discussing classified information up to the Secret/Restricted Data (S/RD) level, and are not TEMPEST protected areas. The following controlled articles may be authorized within such DOE HQ areas, subject to the restrictions outlined below:

- Government and personally-owned cell phones
- Personal digital assistants

- Smartphones and Blackberry-type devices
- eBook readers without cellular capability
- iPod/MP3 type devices.

Although these devices may be taken into an LA, these devices must be removed from the area, have their batteries removed if possible, or turned off and placed in an approved radio frequency (RF) attenuation container (called an RF bag or box) whenever classified material is being processed or discussed. Electronic devices are not authorized in VTRs, Top Secret LAs, Sensitive Compartmented Information Facilities (SCIFs), TEMPEST Protected Areas, or areas where Special Access Program information is stored, processed, or discussed.

Your HSO can give you additional information on the use of cell phones and other electronic devices.

Information Security

DOE HQ is responsible for the protection of a vast array of material, data and intellectual property that is vital to our economic and national security interests. This information includes both classified information and controlled unclassified information (CUI).

Classified Matter Protection and Control (CMPC)

Classified information and matter that is generated, received, transmitted, used, stored, reproduced, or destroyed must be properly protected and controlled to ensure that such matter is not lost or compromised.

DOE uses a graded approach to protection – that is, the level of effort and resources expended to protect a particular safeguards and security interest is commensurate with the effect of its loss, theft, compromise, and/or unauthorized use. Interests whose loss, theft, compromise, and/or unauthorized use would have serious impacts on national security; and/or the health and safety of DOE and contractor employees, the public, or the environment; and/or DOE or other government programs must be given the highest level of protection.

The classification level, category, and other attributes of the information determine the degree of protection and control required to prevent unauthorized access:

- There are three Classification Levels: Top Secret (TS), Secret (S), and Confidential (C).
- There are four Classification Categories: Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (TFNI) and National Security Information (NSI).

HQ has established controls to prevent, deter, and detect unauthorized access to classified matter. Buildings and rooms that contain classified matter are designed to prevent unauthorized physical, visual, and/or aural access to that matter, and classified matter custodians and authorized users are responsible for protecting classified information and classified matter.

All personnel whose responsibilities include generation, handling, using, storing, reproducing, transmitting, and/or destroying classified matter must receive initial and refresher CMPC training and/or briefings, commensurate with these responsibilities.

Classified matter must be processed, handled, and stored in Security Areas that provide protection measures equal to or greater than those in an LA unless an equivalency or exemption is granted based on a vulnerability assessment and an informed risk management decision. Appropriate physical security and access control measures must be applied to each area or building within a Security Area where classified matter is handled or processed.

Need-to-Know

Classified information may be disclosed only to individuals who have the appropriate access authorization (security clearance) for the level and category of information involved, have received all required formal access approval(s), and have a legitimate need-to-know.

An authorized holder of classified information or CUI determines the prospective recipient's need to know – that is, whether the prospective recipient requires access to specific classified or CUI in order to perform or assist in a lawful and authorized governmental function.

Access and Use

Personnel who are granted access to classified matter are personally responsible for the protection of the matter. Classified matter may only be used within approved Security Areas and must be stored in approved storage locations. Personnel must ensure that classified information is marked appropriately with the required classification markings, that appropriate cover sheets are used, and that classified matter is never left unattended. Personnel must electronically process, store, and/or print classified matter only on equipment specifically accredited at a classification level and category equal to or higher than the classified matter being processed. Before sharing classified information with others, the holder of the information must confirm that the person(s) has an appropriate access authorization (i.e., equal to or higher than the classified information) and has a valid need-to-know.

Each HQ organization that possesses classified information has established one or more Classified Document Control Stations that prevent unauthorized access to or removal of classified information. They function as the organization's "gateway" through which all incoming and outgoing classified information must transit to ensure proper transmission, accountability, packaging, receipting, etc.

Line management must designate in writing the individuals within their organization who are authorized to approve employees to hand-carry or escort classified matter. Hand-carrying of classified matter must meet stringent requirements prior to approval, including a Hand Carry Briefing for the carrier that includes emergency contingency plans.

The removal of classified matter from approved facilities to private residences or other unapproved places (e.g., hotels or motels) is prohibited.

Storage

When not in use, classified matter must be stored in a General Services Administration (GSA) approved security container or VTR. Storage in a locked desk drawer is not an approved manner of storage.

All security containers and VTRs must be kept locked when not under the direct supervision of an authorized/cleared individual.

HQ has established a check system to ensure that classified matter is properly stored and that security containers and VTRs are secured at the end of each day or shift. An authorized person in the work area must annotate a Security Container Check Sheet (Standard Form 702) to record openings/closings and end-of-day checks. Additionally, an Activity Security Check List (Standard Form 701) or an equivalent form must be used as a means of checking end-of-day activities for a particular work area where classified activities are authorized.

Accountable Matter

Some classified matter must be entered into an accountability system that provides an audit trail through the use of a verifiable inventory and the establishment of a custodial chain. Accountable matter includes Top Secret matter; Secret/Restricted Data approved for storage outside a Limited Area or higher; and any matter designated as accountable by national, international, or programmatic requirements, such as Sigma 14 and North Atlantic Treaty Organization (NATO) Atomal.

The HQFMSP provides detailed requirements for marking, accountability and control systems, reproduction, receipt, transmission, and destruction.

Classification Review

If you originate or modify a document that may end up being classified, it is your responsibility: (1) to ensure the document is marked with the highest potential overall classification level and category that is likely to be contained in the document until it is formally reviewed, (2) to properly protect and store the document, and (3) to ensure that access to the document is limited to only authorized cleared individuals.

If the potentially classified document that you originate or modify is not intended for public release, whether in paper or electronic format, you must have it reviewed by a Derivative Classifier. If the document *is* intended for public release, you must have it reviewed by the local Classification Officer (at HQ, this is the Director, Office of Classification). In either case, you must have the document reviewed for classification before it is

finalized, released outside of the activity (e.g., ad hoc working group) or office, or filed. The document must be formally reviewed no later than 180 days after its creation – 30 days for a Top Secret document.

If you need to have a classified document reviewed for possible declassification or downgrading, submit the document to your organization's Derivative Declassifier. A Derivative Declassifier review is required even if the document contains a declassification date or event that has passed.

If you believe that any information or document was improperly classified, you are encouraged and expected to challenge its classification status. Contact the Office of Classification for the appropriate steps to take.

Never discuss information that you think might be classified with uncleared individuals, even if the information is in the public domain. The fact that classified information has appeared publicly does not make it unclassified.

Contact your organization's HQ Classification Representative, the Classification Outreach Hotline, (301) 903-7567, or your organization's HSO for additional information.

Controlled Unclassified Information

Within DOE, CUI is information that does not meet the criteria for classification, but that falls under the definition of either Unclassified Controlled Nuclear Information (UCNI) or Official Use Only (OUO). UCNI and OUO are protected through marking, access control, physical protection, and other requirements that restrict reproduction, transmission, destruction, and dissemination.

Unclassified Controlled Nuclear Information (UCNI) is certain unclassified but sensitive information concerning the design of nuclear weapons and their components, or the design and security of facilities that produce or utilize special nuclear materials, the distribution of which is controlled under the Atomic Energy Act.

Official Use Only (OUO) information is certain unclassified information that may be exempt from release under the Freedom of Information Act (FOIA) and has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE-authorized activities.

While there are several categories of OUO information, one category merits special attention: Personally Identifiable Information (PII). PII is OUO and, as such, must not be released to anyone who does not have a legitimate need to know the information.

PII includes:

- An individual's social security number or date of birth
- An individual's medical conditions or criminal history
- Personnel matters in which administrative action, including disciplinary actions, may be taken
- An employee's performance evaluation rating
- An evaluation of a candidate for employment or security clearance.

If you have questions about the protection of PII, call the Office of the Chief Information Officer, (202) 586-0166.

Other-Agency Controlled Information is CUI created by other government agencies. Examples include Department of Defense “For Official Use Only” (FOUO) and State Department “Sensitive but Unclassified” (SBU). These other Agencies’ markings are usually equivalent to DOE’s OUO markings, and documents with such markings may usually be protected as OUO. However, some other-agency CUI may require special handling [e.g., Safeguards Information, Sensitive Security Information (SSI)]. If you are not sure whether certain OUO measures provide equivalent protection, contact the originating agency.

CUI is also used to describe information that will be identified and safeguarded under Executive Order (E.O.) 13556, Controlled Unclassified Information. E.O. 13556 mandates a uniform, government-wide program to identify and protect sensitive but unclassified information. At this time, policies for CUI under the E.O. are still being developed. No timetable has been set for implementation, and implementation will take place over a period of years. Until a national directive is issued and DOE issues its own implementing directive, DOE personnel must continue to follow the requirements for UCNI and OUO information.

Incidents of Security Concern

Incidents of Security Concern are actions, inactions, or events that are believed to:

- Pose threats to national security interests and/or Departmental assets
- Create potentially serious or dangerous security situations
- Have a significant effect on the safeguards and security program's capability to protect DOE safeguards and security interests
- Indicate the failure to adhere to security procedures
- Illustrate that the system is not functioning as designed by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile acts, etc.).

Incidents require follow-up to:

- Ensure that management is aware of the situation
- Determine the facts and circumstances of the incident
- Ensure that corrective actions are taken to mitigate the incident
- Develop actions to correct underlying weaknesses and prevent recurrence
- Document whether issuing a security infraction or taking other disciplinary action is appropriate.

HQ personnel must promptly report suspected Incidents of Security Concern to the Office of Physical Protection (HS-91). Initial reporting may be verbal and is normally performed by the discovering

organization's HSO. It may also be performed by any concerned individual by contacting a Protective Force Officer or by contacting HS-91 staff.

If you discover a potential incident of security concern that involves improper control of classified matter or other security interests, make a reasonable effort to safeguard the security interest if you can do so without putting yourself at risk. For example, you should pick up and safeguard unprotected classified matter or secure a classified repository, but you should not attempt to interrupt an ongoing criminal act.

An Inquiry Officer will be assigned if an incident requires formal follow-up, as determined by the HQ Security Incident Program Manager (HSIPM).

The Inquiry Officer's first priority is to ensure that actions are taken to mitigate the incident – for example, that documents are secured or e-mail servers are sanitized. Once mitigating actions are complete, the Inquiry Officer endeavors to determine the cause of the incident and the actions needed to address any underlying weaknesses. The Inquiry Officer also recommends appropriate follow-up actions, such as retraining, issuance of a security infraction, or other disciplinary action.

If the Inquiry Officer believes that a criminal act may have occurred or that an agent of a foreign power is involved, the Inquiry Officer immediately ceases the inquiry and notifies the HSIPM, who refers the matter to the appropriate law enforcement agencies.

Operations Security (OPSEC)

OPSEC is a process designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive Departmental activities or information and to prevent the inadvertent disclosure of such information.

The goals of the Headquarters OPSEC Program are to provide management with the information required for sound risk management decisions concerning the protection of sensitive information by identifying Critical Information and Indicators that may be of use to an adversary, then recommending cost effective countermeasures to protect that information, and at the same time, developing OPSEC security awareness throughout the HQ complex.

Security Awareness

The Security Awareness Program is established by DOE Order to inform individuals of their safeguards and security responsibilities and to promote continuing awareness of good security practices. To do so, the DOE HQ Security Awareness Program provides the following required briefings: initial security briefing, comprehensive security briefing, the Annual Security Refresher Briefing, and the Security Termination Briefing. Additionally, the Security Awareness Program Manager develops and publishes various informational security pamphlets, posters, newsletters, e-mail notifications, etc., for distribution to DOE HQ personnel. Additional information on the Security Awareness Program can be found at:
https://powerpedia.energy.gov/wiki/Security_Awareness

Headquarters Security Surveys

A survey is an integrated evaluation of all applicable topics to determine whether the safeguards and security program and processes at a facility or site are operating in compliance with Departmental and national-level policies, requirements, and standards. Surveys are conducted or supervised by Federal security personnel.

The Security Survey Program is required by DOE Order 470.4B and provides a basis for line management to make decisions regarding safeguards and security implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities. Surveys also identify safeguards and security program strengths and weaknesses.

There are four types of surveys. An Initial Survey is conducted when a facility clearance is first established. Periodic Surveys are conducted at established facilities at predetermined frequencies. Special Surveys are conducted at facilities for specific, limited purposes, and finally, Termination Surveys are conducted when a facility or activity closes to verify the proper termination of Departmental activities and appropriate disposition of safeguards and security interests.

Technical Surveillance Countermeasures (TSCM)

The objective of the TSCM Program is to detect and/or deter a wide variety of technologies and techniques that can be used to obtain unauthorized access to classified and sensitive unclassified information. The HQ TSCM Program provides expert technical and analytical capabilities to detect, nullify, and isolate electronic eavesdropping devices, technical surveillance penetrations, technical surveillance hazards, physical security weaknesses, and technical education awareness information, within DOE HQ areas of operations.

Types of services performed: surveys, inspections, monitors, advice and assistance, special TSCM services, educational/awareness briefings, and gift inspections.

The TSCM Program also investigates Technical Surveillance Countermeasures Incidents:

- Any discovery of a possible or actual technical surveillance penetration
- Any discovery of a condition that could permit technical surveillance of an area through equipment that, by reason of its normal design, installation, operation, or component deterioration, allows transmission of information
- Any use of electronic surveillance equipment by persons not authorized to conduct electronic surveillance.

The fact that an area is scheduled for or has received a TSCM service is classified. Precautions must be taken to preclude OPSEC indicators that could reveal a TSCM team is scheduled to be, or has already been, in the area.

What to do if you suspect that you have DISCOVERED A DEVICE:

- DISCREETLY cease all classified conversation and activity.
- DO NOT SAYOUT LOUD that there is a suspect device in the area or discuss the possible device in rooms above, below, and adjacent to the location.
- SECURE THE AREA where the suspect device is located to prevent anyone from removing it.
- IMMEDIATELY contact the HQ TSCM Operations Manager (in person) or via secure communications located outside the suspect area.

Foreign Ownership, Control or Influence (FOCI)

The objective of the FOCI Program is to evaluate and adjudicate the foreign involvements of companies being considered for award of a contract that requires access to classified matter. A FOCI determination must be rendered prior to award of the contract and issuance of a facility clearance (see Facility Clearance and Approval Program). If a company already holds a facility clearance issued by another DOE office or another government agency, a FOCI determination is not required.

Facility Clearance and Approval

The DOE Facility Clearance and Approval Program regulates DOE's approval of facilities that are intended to access, receive, generate, reproduce, store, transmit, or destroy classified information or matter. This approval is required for DOE-owned sites, contractor facilities, and other government agency facilities. Facilities are registered using DOE Form 470.2, Facility Data and Approval Record, and facility clearance and approval information is tracked in the Safeguards and Security Information Management System (SSIMS).

SSIMS also tracks all contractual agreements that require access to classified matter by contractors. Before a contractor can request access authorizations ("Q" or "L" clearances and badges) for its employees, the interest (contract, subcontract, work for others agreement, interagency agreement, etc.) must be registered in SSIMS.

SSIMS is also the database for tracking the classified mailing addresses for approved facilities that can receive and store DOE classified matter. Before classified matter is sent, whether by regular mail, express mail, or hand carrying, the sender must verify the receiver's classified mailing address in SSIMS.

HQ Equivalencies and Exemptions

DOE security orders and manuals often require that certain measures be taken to protect DOE security interests. In some cases, a DOE organization may be unable to comply with the requirements as specified in the directive, but can achieve the security goal in another equally effective manner. In other cases, the security requirement cannot be met as prescribed.

DOE Order 251.1C, *Departmental Directives Program*, Paragraph 6a(3)(c), establishes a process for requesting and approving "equivalencies and exemptions" to the requirements in DOE directives. HQ elements seeking an equivalency or exemption to DOE security requirements as they are implemented at HQ must obtain the approval of the Chief Health, Safety and Security Officer (HS-1) through the Director, Office of HQ Security Operations. All approved equivalencies and exemptions at HQ must be entered into the SSIMS database.

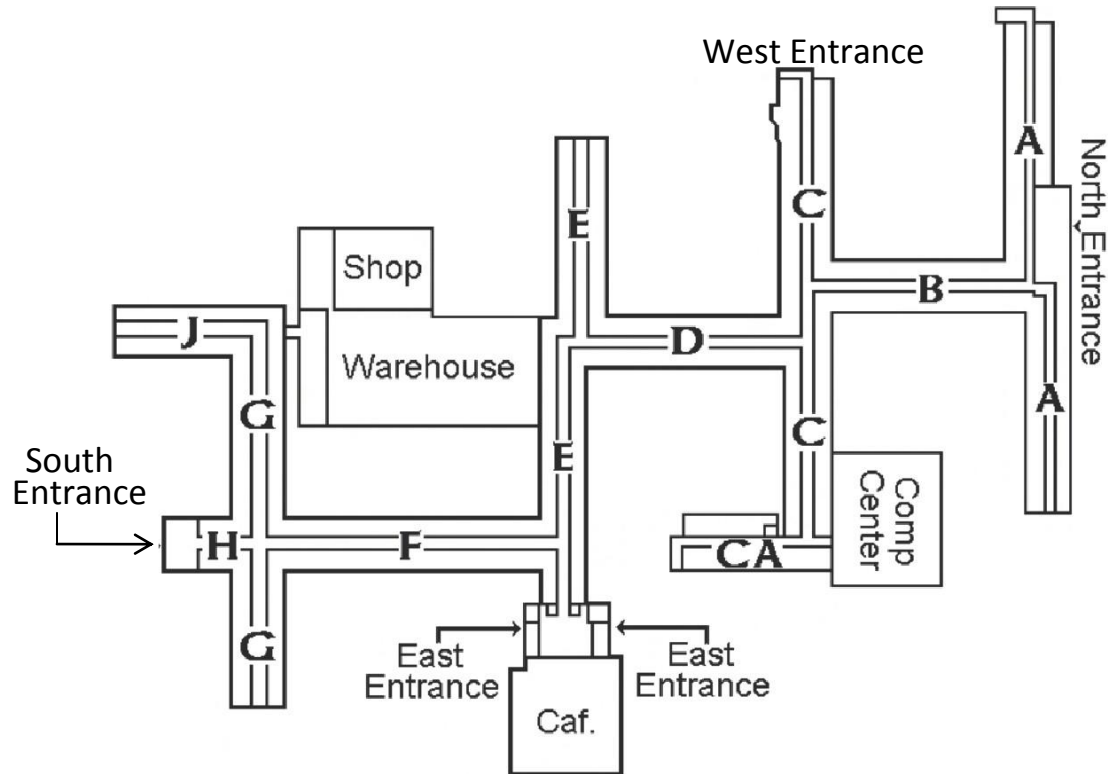
HQ Security Program Contacts, Facility Diagrams, and Bus Schedule

Emergency Contacts Protective Force/Central Alarm Stations	
Non-Emergency - Germantown	301-903-2403
Emergency - Germantown	166
Non-Emergency - Forrestal	202-586-6900
Emergency - Forrestal	166
Non-Emergency - Cloverleaf	301-903-2403
Emergency - Cloverleaf	9-911
Non-Emergency - 950 L'Enfant Plaza	202-863-7901
Emergency - 950 L'Enfant Plaza	9-911
Non-Emergency - 955 L'Enfant Plaza	202-586-9384
Emergency - 955 L'Enfant Plaza	166

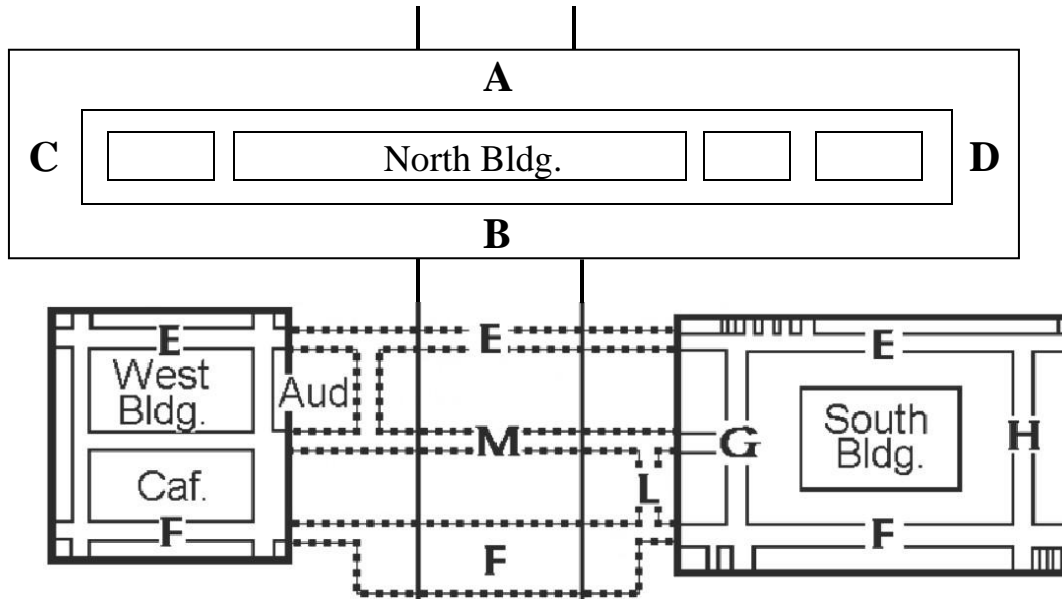
Security Program Contacts	
Area of Expertise	Phone #
HQ Office of Information Security	
Director	301-903-9990
Security Awareness	301-903-7189
FOCI/Facility Clearance and Approval/Deviations	301-903-5287
Headquarters Security Surveys/Security Area Approvals	301-903-9987
	301-903-5688
Classified Matter Protection and Control	301-903-9986
OPSEC	301-903-4031
HQ Technical Security Program	
Director	301-903-9992
Technical Surveillance Countermeasures	301-903-9992
	301-903-9221
	202-586-5775
HQ Office of Physical Protection	
Director	202-586-7887
Forrestal Facility Security Manager	202-586-2680
Germantown Facility Security Manager	301-903-0145
950 and 955 L'Enfant Plaza Facility Security Manager	202-586-2680

Office of Headquarters Personnel Security Operations	
Director	301-903-4175
Personnel Security - HQ Security Clearance Issues	301-903-4175
Personnel Security - Personal Identity Verification (PIV) and HSPD-12	301-903-4175
Office of Classification	
Identification of Classified, UCNI, and OUO Information	301-903-7567
Badging	
Germantown Badging Office	301-903-3330
Forrestal Badging Office	202-586-5764
Cyber Security Program	
Associate Chief Information Officer for Cyber Security	202-586-0166
HQ DAA for unclassified systems	301-903-2659
HQ DAA for classified systems	301-903-2659
Deputy Associate CIO for Cyber Security	202-586-9805
HQ ISSM for classified systems	202-586-6691
For HQ IT and Cyber Security Issues - HQ Hotline	301-903-2500
Cyber Forensics Lab	202-586-8139
DOE-Computer Incident Response Capability (DOE-CIRC)	866-941-2472
Inspector General	
Hot Line	202-586-4073
Intelligence/Counterintelligence	
Eric Jackson (Security Related Matters)	202-586-1127
Bob Thompson (Counterintelligence Incident Reporting)	301-903-0434

Germantown Building Diagram



Forrestal Building Diagram



DOE Shuttle Bus Schedule	
Departs	Arrives
7:00 a.m.	8:30 a.m.
8:45 a.m.	10:00 a.m.
10:15 a.m.	11:15 a.m.
11:30 a.m.	12:30 p.m.
1:15 p.m.	2:30 p.m.
3:00 p.m.	4:15 p.m.
5:00 p.m.	6:15 p.m.
Current as of September 2012	

DOE HQ Security Conditions (SECON) System

DOE Order 470.4 B, Appendix A, Section 1, Chapter II, identifies five Security Conditions, or SECONs, which departmental facilities must plan for. They range from SECON 5 (the lowest) to SECON 1 (the highest):

- SECON 5 (*Low Condition*). This condition is declared when there is a low risk of terrorist activity, continuity conditions, or environmental and/or severe weather conditions. SECON 5 exists when a minimal SECON concern exists but warrants only a routine security posture.
- SECON 4 (*Guarded Condition*). This condition is declared when there is a general risk of terrorist activity, continuity conditions, or environmental and/or severe weather conditions. SECON 4 applies when there is a broad, non-specific threat of a possible event, the nature and extent of which are unpredictable. All measures selected for use under SECON 4 must be capable of being maintained indefinitely.
- SECON 3 (*Elevated Condition*). SECON 3 is declared when there is a significant risk of terrorist activity, continuity conditions, or environmental and/or severe weather conditions. SECON 3 applies when an increased and more predictable threat against DOE facilities exists. The measures used in SECON 3 must be capable of being maintained for lengthy periods without causing undue hardship, affecting operational capability, or aggravating relations with the local community.

- SECON 2 (*High Condition*). SECON 2 is declared when there is a high risk of terrorist activity, continuity conditions, or environmental and/or severe weather conditions. This condition may apply when an incident occurs or intelligence is received indicating that some form of action against DOE personnel and facilities is imminent. Implementation of measures in this security condition for more than a short period will probably create hardship and affect the routine activities of the facility/site and its personnel.
- SECON 1 (*Severe Condition*). This condition reflects a severe risk of terrorist activity, continuity conditions, or environmental and/or severe weather conditions. SECON 1 applies in the immediate area where conditions have occurred that may affect a DOE facility/site or when an attack is initiated on the facility/site. Implementing SECON 1 will create hardship and affect the activities of the location and its personnel. Normally, this condition will be declared as a localized response.