SEC101

COUNTERINTELLIGENCE, CLASSIFICATION, EXPORT CONTROL AND SECURITY

REFRESHER BRIEFING

Introduction

The Laboratory depends on a knowledgeable and vigilant workforce
in order to keep all of our information safe and secure.

- This course will provide you important information about your responsibilities in the areas of counterintelligence, classification, export control and security.
- You can find the helpful materials and links on the last page of this document.
- The course is divided into **4 Modules** - Counterintelligence, Classification, Export Control and Security and should take about 30 minutes to complete.

Module 1 – Counterintelligence

Counterintelligence is information gathered and activities conducted to detect and protect against espionage, other intelligence activities, sabotage, or assassinations conducted for, or on behalf of, foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical document or communications security programs.

Upon completion of this module, you will be able to:

- Explain the mission of the Argonne Office of Counterintelligence
- Describe the foreign intelligence threat to Argonne
- Outline your hosting responsibilities
- Identify methods of targeting used overseas
- Recognize possible espionage indicators
- Identify cyber threats and their reduction methods
- Identify your reporting requirements
- Locate additional information related to counterintelligence

Argonne Office of Counterintelligence - Our Mission

- **Detect, deter, and counteract** attempts of foreign powers to illegally obtain information from the Laboratory
- **Educate employees** to be vigilant and aware of possible counterintelligence threats
- **Work closely with agencies** responsible for protecting the United States from threats from hostile powers, terrorists, and terrorist organizations
- **Conduct activities** in a professional manner, sensitive to the needs of Argonne employees

International Environment

Globalization is rapidly changing international competition. Foreign Governments and businesses seek U.S. information to establish a competitive advantage.

Governments compete for reasons such as:

- Political ideology
- National security
- Economic prosperity
- Influence
- Resources
- Territory

International collaboration, which is essential today, makes intelligence gathering easier for foreign governments. Information has greater value in a digitized world. Competitive advantages are leveraged through information.

Intelligence Collection

To obtain information from foreign countries, governments maintain professional intelligence and security services; almost every country collects information in this way.

Intelligence organizations task their employees, and sometimes private citizens, to collect U.S. valued information.

Valued Information or information sought after includes:

- Military/Defense
  "Classified" material
- Political
- Economic
- Science/technology even if later published, to get a head start
- Business
  sensitive, proprietary, intellectual property

Unlike the U.S., foreign intelligence organizations offer the information they collect to businesses in their country which gives them an (unfair) advantage in the market.

Foreign Intelligence Threat

Factors that increase the possibility that you or other Argonne employees will be targeted are:

- Your access to information people, or places of active intelligence interest
- Ethnic, racial or religious background that may attract the attention of a foreign intelligence operative
- Work in a position or geographic location in the U.S. where it is easy for foreign nationals to gain access to you

Possible Espionage Indicators

- Excessive or habitual alcohol/illegal drug usage or incidents
- Attempts to obtain information without need-to-know; undue curiosity
- Unexplained affluence or lifestyle inconsistent with known income
- Unexplained or excessive use of copying equipment (faxes, copiers, computer media, etc.)
- Unusual foreign travel patterns
- Personal problems; relationships, marital or financial
- Frequently working alone late and on days off
- Unusual desire for recognition
- Correspondence or visits to personnel or establishment of a sensitive country
- Removal of classified/sensitive material from work area
- Misuse of computer/fax/copier
- Criminal or immoral conduct
- Unexplained mood changes

Foreign Travel

Foreign travel presents an operating environment which is conducive to the needs of the intelligence and security services.

Methods of targeting while overseas:

- Secret searches of unattended personal belongings, hotel rooms
- Physical, audio, and technical surveillance
- Blackmail
- Elicitation and cultivation techniques
- Solicitation
- Close and continuing relationships

Visits

Argonne National Laboratory is a leader in the development of new and advanced technologies. To maintain its competitive status in the development of new technologies, Argonne often searches out individuals and programs from both international and domestic organizations with the desirable scientific and technical skills, and establishes collaborative ventures to achieve such goals.

These collaborative efforts are essential to capturing benefits of scientific and technical advances as well as furthering mutual agreements. There are, however, inherent risks to such collaborative efforts.

Site visits provide low cost and low risk opportunities to gain access to needed technologies for visitors. While most visitors are here in genuine pursuit of collaborative technological efforts, there are those visitors who maintain hidden agendas.

Indicators of Intelligence Tasking

A visitor who:

Attempts to solicit information outside the stated scope or intent of the visit/assignment; specifically, if the request for information may involve classified or sensitive information (need-to-know)

Need-to-know - A determination made by an authorized holder of classified or unclassified controlled information that a prospective recipient requires access to specific classified or unclassified controlled information in order to perform or assist in a lawful and authorized governmental function.

"Wanders" away from his normal working space specifically identified in the security plan, and is offended when challenged about his presence in "unauthorized" locations

Does not exhibit similar levels of expertise as other members of the group, does not appear focused on the agenda of the visit, or engages in incongruous behavior for the occasion

Attempts to access programs, data, or applications beyond the computer access specifically approved by the host organization

Host Responsibilities

In all cases, hosts are responsible for ensuring that site access requirements are met, and are responsible for the actions of their visitor. As a host, you are also responsible for ensuring visitor compliance with all environmental, health, safety, and security requirements of the site.

The Laboratory reserves the right to take appropriate disciplinary actions for failure to adhere to all requirements for the admittance and hosting of visitors on site.

As a host, you should also assure that:

- The subject matter of the visit is clearly understood.
- Determine the areas of your work that may be sensitive, but not classified, and could potentially shed light on classified work.
- The security plan for the visit is clearly understood and followed, thus ensuring that visitors do not receive unauthorized access to information or locations.

Hosts are required to report requests for information, outside the stated scope or intent of the visit, or any suspicious behavior.

Internet Threats

Information stored on an organization's internal networks, typically available to inside users, has been successfully exploited by the Foreign Intelligence Services (FIS) and other foreign collectors.

U.S. Intelligence Community (USIC) and law enforcement reports have established that Foreign Intelligence Services (FIS) and other foreign collectors aggressively seek to exploit government and industry information available on the Internet, including information on web pages.

Information stored on an organization's internal networks, typically available to inside users, has also been successfully exploited.

Cyber Threats

Outsider threats range from the hacker using social engineering techniques and network scans to gain access to computers and networks, to the Foreign Intelligence Services collectors recruiting system administrators and network managers to gather information for them.

Argonne **insider threats**, which involve the misuse of authorized privileges, have long presented serious problems for government and private sector computer systems and may be more difficult to identify.

Reduce Cyber Threats

Cyber attacks can happen at home, at work or while on travel.

Travel

- Don't take any portable computer equipment or handheld organizers on foreign travel - business or pleasure.
- If there is a requirement to take a laptop on a trip, try and get one from a pool of generic computers within your division.
- Have your equipment examined upon your return by a computer security or technical representative.
- Have an image made of the system before your trip.
- Never leave your portable equipment unattended.

Internet

- Be aware that visiting a web site containing malicious software may cause software to be downloaded and installed on your computer.
- Be aware of social engineering, elicitation, and recruitment techniques, and report attempted contacts to the Argonne Counterintelligence Office.
- Report any suspicious network activity that appears to have a foreign origin to cyber@anl.gov.

Email

Receiving unsolicited e-mail from foreign countries, to include those considered sensitive by the Department of Energy (DOE), is a common occurrence at Argonne.

These e-mails usually constitute some type of request by the foreigner, such as information about employment opportunities or even specific technical information. The Counterintelligence Office would like to review these types of messages before a response is sent.

Forward copies of all unsolicited e-mail messages received from foreign countries to cyber@anl.gov for a review by the Cyber Group.

Questions regarding unsolicited e-mail messages from foreign countries may be directed to the Cyber Specialist (link to all Counterintelligence Contacts can be found under the Resources, at the top right of the screen).

Why do the Insiders spy?

The Insiders can spy for the following reasons:

- They were volunteered or recruited to spy
- They had a character weakness
- One or more of the four foundations for espionage existed:
    - Opportunity
    - Motive
    - Ability to overcome inhibitions
    - Triggers to set the betrayal in motion

All U.S. spies were at one time a trusted friend or co-worker. However, because of the reasons listed, they violated that trust.

What should you do?

The role of counterintelligence in combating terrorism is to detect, deter, and neutralize information gathering for targeting and assessment of the Department of Energy's programs, facilities, technology, or personnel by terrorists.

Counterintelligence and security have joint interest in domestic terrorist activities. Counterintelligence is focused on those with foreign sponsorship or direction.

Report Unusual Activity

You can help the Security and Counterintelligence by being vigilant and aware of activities that are indicators of a terrorist event. These indicators could provide a warning that saves lives and property. Some of these indicators are:

- Surveillance of the site, its employees and activities
- Unusual and unsolicited interest in personnel and technologies
- Attempts to gain site access by using false documents
- Suspicious behavior, such as nervousness, or wearing inappropriate clothing for the season
- Attempts to challenge security

Protect Technologies and Information

It is YOUR responsibility to protect Argonne's sensitive technologies and information, and to REPORT:

- Contacts with foreign nationals
- Travel to sensitive countries
- Illegal or unauthorized access to classified or sensitive information
- Concerns

When in Doubt

- Report it to your Counterintelligence Office; information will be handled discreetly. You are the key to a successful Counterintelligence program.

Know your reporting requirements. You must report:

- Any indication/suspicion of theft of Argonne technologies
- Any indication of targeting of Argonne employees, technologies, or programs
- Any attempt to solicit classified or sensitive information without a valid need-to-know (foreign or U.S. citizens)
- Any enduring substantive relationships with sensitive country foreign nationals (non- permanent resident aliens) that involve sharing of personal information or the formation of emotional bonds
- Any foreign travel for which foreign monetary support is provided
- Substantive business transactions with citizens of sensitive countries (Financial support provided to family members is not included)
- Anomalies (things that just make you feel suspicious or uncomfortable)

Counterintelligence Website

Please note that you may always refer to the Counterintelligence website for more information.

For your reference, link to the website and other helpful materials can be found on the last page of this document.

The website includes:

- Counterintelligence fact sheets, publications and links
- Information on foreign travel and alerts
- Information on foreign national access
- General counterintelligence information
- Reporting requirements

Module 2 - Classification

Classification is the identification of information that needs to be protected in the interests of national security.

It is the act or process by which information or matter is determined to require protection in the interest of national security under either the Atomic Energy Act of 1954, as amended, or the Executive Order 13526.

Upon completion of this module, you will be able to:

- Define classification
- Identify your responsibilities regarding classification of information
- Describe penalties for violating classification requirements

Why is it important?

Unauthorized disclosure, loss, misuse, alteration, or destruction of classified information may adversely affect national security or governmental interests.

This information requires protection and control as mandated by statutes, regulations, Executive Orders, government-wide and the Department of Energy (DOE) policy and directives.

All employees are required to understand the regulations associated with classified information.

Classification Levels

Classification levels are a designation assigned to specific elements of information based on the potential damage to national security if disclosed to unauthorized people.

The three levels in descending order of potential damage are:

1. Top Secret - Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security
2. Secret - Unauthorized disclosure could reasonably be expected to cause serious damage to the national security
3. Confidential - Unauthorized disclosure could reasonably be expected to cause damage to the national security

Through classification, Argonne protects important information, thus preventing its compromise (i.e., restricting its availability to adversaries), yet allowing its use by individuals who have the appropriate clearance and need to know.

What are your responsibilities?

All employees who work, or plan to work, in subject matter areas that may be classified are required to obtain classification reviews of:

- Their planned work before beginning to document that work.
- All documents, before releasing them outside Argonne.

Examples of “documents” include, but are not limited to, informal white papers, concept papers, and pre-proposals; formal funding proposals; abstracts; publications; posters, and presentations. Unclassified documents are also subject to the publication release and clearance process established in the SCITECH - series of policies and procedures.

Don’t assume that information is unclassified merely because it may be on the Internet, publicly available or in open sources.

Contact your Derivative Classifier (DC) or the Classification Officer if you have any questions or concerns regarding the use of open source information in Argonne documents.

You are responsible for knowing that unclassified information can become classified when combined with other unclassified information.

The use of information from inappropriate and unofficial sources in the development of official documents is especially risky because unauthorized publications may contain classified information.

Pertinent Laboratory Policies and Procedures

The Policies and Procedures listed here include mandatory actions if the proposed work involves potentially classified subject matter areas.

LMS-POL-19 - Protection of National Security and Other U.S. Interests

Establishes Argonne's policy regarding protection of classified information and controlled unclassified information.

All employees are responsible for appropriately handling information for which such controls exist.

LMS-PROC-75 - Protecting Information in the Project Lifecycle

Establish the process for protecting classified information and controlled unclassified information (CUI) the project lifecycle (including proposals & pre-proposals) for funding from U.S. Department of Energy (DOE) and non-DOE sponsors.

LMS-PROC-105 - Strategic Partnership Projects Proposals

Establishes the process for preparing, approving, and submitting Strategic Partnership Projects Proposals to prospective sponsors outside the U.S. Department of Energy (DOE).

Penalties and Violations

Per the Code of Federal Regulations (10 CFR Part 824), Argonne can be subject to a civil penalty of up to **$110,000 per day for each offense** for violating any rules, regulations, or orders relating to the safeguarding or security of restricted data or other classified information.

Violations are assigned a severity level.

Other factors to be considered include the frequency and willfulness of the violation, and whether appropriate and effective corrective measures have been taken to resolve the problem.

The rule also provides for reduction of any proposed civil penalty when the violation is self-reported.

Title 10, Code of Federal Regulations, Part 824 stipulates that a contractor or subcontractor to the Department of Energy (DOE) who violates any rule, regulation, or order relating to the safeguarding or security of Restricted Data or other classified information shall subject Argonne to a civil penalty up to $110,000 per day for each offense.

DOE has the responsibility for enforcing this regulation as it applies to DOE contractors and subcontractors.

Examples of Major Classified Subject Matter Areas

Uncleared employees have the potential to engage in research that involves potentially classified subjects, such as:

- Nuclear Weapon Design
- Nuclear Weapon Military Utilization
- Nuclear Material Use and Production

- Improvised Nuclear Device (IND)
- Radiological Dispersal Device (RDD)
- (certain) Nuclear Reactors
- Critical Infrastructure
- Nuclear Emergency Support Team (NEST)
- Intelligence/ Counterintelligence
- Foreign Government Information (FGI)
- Non Proliferation Safeguards and Security
- Vulnerabilities related to National Security

Managers are responsible for ensuring that personnel under their supervision receive briefings that explain which types of information or research have the potential to be classified.

When should you obtain a review?

All employees, those with or without a security clearance, are required to obtain reviews of all work that is conducted in a potentially classified subject matter area. **Prior to commencing work,** a review should be conducted.

- **BEFORE** you begin developing hard copy/electronic information
- **BEFORE** you begin compiling information/documents from open/public electronic sources (e.g. Internet)

Additional Information

Always consult a Derivative Classifier (DC) prior to beginning work on a project in a classified subject area and as the project progresses.

Inform the DC about the project's scope, internal and external organizations involved and any associated classification concerns.

Contact the:

- Classification Officer or the
- Classification Analyst

to request clarification of issues or questions which may not have been resolved by a Derivative Classifier.

Classification Services Website includes links to helpful resources, such as:

- General Classification Guidance for Employees
- Classification Briefing
- Official Use Only Briefing
- DOE Orders/Directives
- LMS-POL-19 - Protection of National Security and Other U.S. Interests
- LMS-PROC-75 - Protecting Information in the Project Lifecycle
- LMS-PROC-105 - Strategic Partnership Projects Proposals

Information Security

Information Security is the protection and control of classified and controlled unclassified information. Unauthorized disclosure, loss, misuse, alteration, or destruction may adversely affect national security or governmental interests.

As mentioned earlier, this information requires protection and control.

Official Use Only (OUO) is controlled unclassified information within the Department of Energy, and may be exempt from public release under the Freedom of Information Act (FOIA).

Common examples include:

- Personally Identifiable Information (PII)
- Export controlled information

Anyone who needs OUO information to perform his or her job or other DOE-authorized activities, may access OUO documents.

You are responsible for protecting against access to OUO information by those who do not need it for official activities.

Sensitive Information

The following types of sensitive information at Argonne are also of interest to certain competitors:

- Military or National critical technologies
- Proprietary and business sensitive information technology
- Foreign government information

Sensitive Information includes both classified and unclassified information and matter. While classified information has clear and defined protection measures, controlled unclassified information is not afforded the same level of protection. This allows an adversary a greater opportunity for collecting information.

Operations Security (OPSEC) is a countermeasures program to prevent foreign intelligence agents, criminals, terrorists, or other adversaries from obtaining classified, critical, or controlled unclassified information about our programs and activities.

Understanding the value of sensitive information, and taking steps to protect that information from inadvertent release, is the principal function of the program.

Controlled Unclassified Information is information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U.S. government.

Governmental interests are those related, but not limited to, the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law- enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. government by its citizens.

Security Incidents

Security incidents include a range of possible actions, inactions, or events that:

- Pose threats to national security interests and/or departmental assets;
- Create potentially serious or dangerous security situations;
- Have a significant effect on the Safeguards & Security (S&S) Program's capability to protect Department of Energy's S&S interests;
- Indicate the failure to adhere to security procedures; or
- 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 of security concern can occur in the following subcategories:

- Information security
  Classified Matter Protection and Control and National Security Systems
- Nuclear material control and accountability
- Personnel security
- Physical protection
- Protective force

Reporting an Incident

Any person who observes, finds, or has knowledge or information about a potential incident of security concern must immediately report this information.

Loss, mishandling, compromise, unauthorized disclosure, and unaccounted-for classified matter shall be handled according to applicable Department of Energy Orders.

Upon discovery or notification, **immediately contact** one of the individuals listed on the right. This notification must be **a direct phone contact**, not a message left on voice mail.

For specific reporting times required, see DOE O 470.4B, Safeguards and Security Program (linked on the last page of this document).

Contacts:

Facility Security Officer
Kim Mandekich
Office (630) 252- 9600
Cell (630) 863-3053

If no contact can be made with the Facility Security Officer listed above, contact: Protective Force (630) 252-5730

Module 3 – Export Control

Export Control Regulations contain sets of rules used in determining the proper export licensing requirements of various commodities and technologies.

These Federal Regulations exist to allow international commerce while maintaining the well-being and national security of the United States.

The main export control regulating departments are:

- Department of State
- Department of Energy
- Department of Commerce
- Department of the Treasury

Department of State - regulating military technology, equipment, and intelligence advantages under the International Traffic in Arms Regulations (ITAR). Often identified as ITAR U.S. Munitions List (USML) Categories.

Department of Energy and Nuclear Regulatory Commission - regulating nuclear technology, materials, and equipment under 10 CFR 810 and 10 CFR 110 regulations.

Department of Commerce - regulating technology, materials, software, and equipment that has both commercial and military applications, (often referred to as dual-use) under the Export Administration Regulations (EAR). Often identified with an Export Control Classification Number (ECCN) (examples: 4A994, 3E001, EAR99).

Department of the Treasury - regulating embargoes and economic sanctions under the Trading with the Enemy Act and other specific sanction lists.

Upon completion of this module, you will be able to:

- Explain Argonne export control regulations, policy and violations
- Locate additional export control information

Export Control Policy - LMS-POL-23

The policy states the following: “Argonne is firmly committed to strict adherence to all U.S. export control laws and regulations. Under no circumstances must the export of technical data, software, or commodities take place contrary to U.S. export control laws and regulations. In addition, the Laboratory also follows U.S. Department of Energy (DOE) policy and executive orders, and these orders agree with the export control laws and regulations.

Sponsorship of Laboratory operations/functions by DOE does not mitigate, supersede, or remove the Laboratory's responsibility to adhere to U.S. export control laws and regulations. Administrative, civil, and criminal penalties exist for violations of export control laws and may be imposed against the Laboratory and/or individual employees. Because of potential serious consequences associated with failing to comply with U.S. export control laws and regulations, all employees must be aware of their obligations for full compliance.”

What is and what is not an Export?

An export is the transmission, shipping, or hand carrying of equipment, materials, items, proprietary software, or controlled information or technology out of the United States or to a foreign person within the United States.

A "deemed export" is the transmission of controlled information or technology to foreign person within the United States.

Before exposing a foreign person to controlled information or technology, be sure to first consult with the Argonne Export Security and Compliance office.

An export of technology can occur when technical information is released to a foreign person or foreign entity where:

- Restrictions are in place for the publication of scientific and technical information resulting from the project or activity.
- The research is funded by the U.S. government or military contractors, and specific access and dissemination controls protecting information resulting from the research are applicable.
- An invention is being protected until the time that a patent is issued, or the information becomes ordinarily published and shared broadly within the scientific community.

Exempt from Export Control

- **Fundamental research**

Basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community.

It is distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

- **Publicly Available Information**

Technology made available to the public without restrictions on its further dissemination, such as through subscriptions, libraries, conferences, meetings, or seminars generally accessible to the public, Internet public dissemination, published patents, submission of manuscript, presentation, imagery, software, or some other representation of knowledge to be made publicly available if accepted for publication.

Scenario 1

You have been invited to present a paper at a prestigious international scientific conference on a subject that is typically export controlled.

Scientists in the field are given an opportunity to submit applications to attend. Invitations are given to those judged to be the leading researchers in the field, and attendance is by invitation only.

Attendees will be free to take notes. Some of the attendees will be visitors from foreign countries.

Do you need an export license for your paper?

Yes, if you are presenting information that is designed, developed, configured, adapted, or modified for a military use.

Yes, if the sponsor of your work has placed restrictions on publication of the information.

No, if none of the above apply, and you are the owner of the information, or the sponsor of the work has granted unlimited distribution of the information.

Release of information at an open conference and information that has been released at an open conference is an act of publishing the information.

The conference described fits the definition of an open conference.

Scenario 2

You work as a researcher at a Government-owned, contractor-operated research center.

Can you share the results of your unpublished research with foreign nationals without concern for export controls?

If your research is designated as Fundamental Research, or Publicly Available Information by any appropriate system devised to control release of information at your research center, it will be treated as such by the export regulations.

Therefore, the research will not be subject to the export regulations, provided no Controlled Unclassified Information or military technology is released.

Otherwise, you would need to request an export control review.

State Sponsors of Terrorism and Embargoed Countries

State Sponsors of Terrorism (SST) and Embargoed countries are those that have U.S. sanctions against them, and nothing should be sent to them without a review by the Argonne Export Security and Compliance office.

The U.S. Department of State designates Cuba, Iran, North Korea and Syria as SST countries.

In addition to the Department of State's SST list, other U.S. Departments such as Commerce and the Treasury's Office of Foreign Assets Control (OFAC) implement additional sanctions on 30 different countries or territories. The entire list of embargoed countries can be found on these department's respective websites.

Exporters and re-exporters should be aware that other U.S. Government agencies administer regulations that could also impact their export or re-export transactions.

Policy Violations and Assistance

Argonne National Laboratory and/or the individual employee may be liable if significant violations of Export Control Regulations occur.

Penalties may include seizure of laboratory equipment, fines and prison terms.

Violations may occur if an export is conducted without the proper Export Control review.

Assistance

The Export Security and Compliance office is here to assist you.

For contacts or more information, you may visit our website. For your reference, the website link can be found on the last page of this document.

Module 4 - Security

Argonne's Safeguards and Security Program protects you and your visitors.

All Argonne employees need to be aware of the security requirements that guide the Safeguards and Security Program in achieving its mission.

Upon completion of this module, you will be able to identify Argonne's security requirements related to

- Incident reporting
- Site access
- Operating a motor vehicle
- Badges
- Hosting visitors
- Onsite events

Reporting Responsibilities

See something - Say something

Call 9-1-1 from an Argonne landline or **(630) 252-1911** from a mobile phone.

Report:

- Theft or destruction of property
- On-site or off-site criminal activity
- Vandalism or malicious mischief
- Civil disorders or demonstrations
- Bomb threats, hoaxes, or incidents
- Any emergencies or suspicious activities

Physical Security

Access to Argonne and its facilities is restricted to employees, contingent workers, DOE employees, on-site contractor personnel, and authorized visitors who have an appropriate site access credential.

All individuals entering Laboratory property are subject to search. Signs are posted at all Laboratory entrances to delineate prohibited articles which cannot be introduced to the site.

The Laboratory prohibits the sale, manufacture, distribution, possession, use or abuse of alcohol or illegal drugs.

Prohibited Articles

Individuals are prohibited from bringing onto the Argonne site:

- Firearms, dangerous weapons or destructive devices
- Explosives or incendiary devices
- Radioactive sources
- Open containers of alcoholic beverages
- Illegal drugs
- Pets or other animals

Controlled Articles

- Portable electronic/recording devices in areas approved for classified work

Operating a Motor Vehicle

Everyone operating a motor vehicle onsite must adhere to all **Illinois Rules of the Road**, such as carrying their driver's license, insurance card, wearing seat belts, etc. The Illinois traffic law is enforced by the Protective Force officers at Argonne.

Illinois Law/ Rules of the Road — and Argonne policy — requires drivers to make a complete stop at all stop signs. A complete stop is defined as a complete cessation from movement. If it is a multi-way stop sign, wait your turn. If the stop sign is hand-held, stop until an authorized person or construction zone flagger signals that it is safe to proceed.

Drivers must yield the right-of-way to approaching traffic and emergency vehicles. When passing bicycles or pedestrians, create a safe separation distance of at least 3 feet. When approaching traffic prevents the proper separation distance, wait for obstructing traffic to pass.

Pedestrians in, or at the edge of established crosswalks, have the right-of-way. Drivers must stop for pedestrians in any crosswalk.

All individuals riding a motorcycle or motor-driven cycle, moped, scooter, roller skates, roller skis, skateboards, e-micromobility device, or bicycle on site must wear a helmet. All helmets must be certified by the applicable agency.

For more information on Traffic Safety, see LMS-POL-6 (link provided on the last page of this document).

Badge Responsibilities

Badges:

- Must be worn at all times while on Laboratory property, on the outermost garment of clothing, on the front portion of the body, from the waist up.
- Must be used for official Laboratory business only.
- Must NOT be worn while off DOE property.
- Must be returned to Division, HR, or Security upon termination.

As a badged employee, remain with your visitor at all times while on site.

Get a new badge if:

- There is a change in your legal name or appearance
- It is damaged or discolored

Lost or stolen badges:

- Must be reported immediately to the Argonne Protective Force, ext. 2-5730.
  In addition, an ANL-994 form needs to be completed for the lost/stolen badge. If a badge is discovered missing during off-hours, it should be reported as soon as possible on the next business day.

Hosting Visitors

Visitors are defined as persons seeking access to the site who are not Argonne/DOE employees or other contingent workers.

All visitors, 16 years of age or older, require a gate pass to enter the site for Laboratory- approved activities.

To receive a gate pass, visitors are required to present a valid form of photo identification. You may contact the Site Access Manager, or review LMS-POL-67 and LMS-PROC-320 for additional information.

Valid Form of Photo Identification – visit the **Site Entry Requirements** page for more information. Link to the site is provided on the last page of this document.

Host Responsibilities

- Advise the visitors to provide notification to the host when the visitor is on site, and remain with them at all times.
- Confirm citizenship of their visitors.
- Notify visitors of general site rules.
- Ensure that the visitors adheres to the general purpose of the visit and that the length and type of approved access (day, night, weekend) is consistent with the purpose of that visit.
- Inform visitors that the gate passes must be worn at all times while on Laboratory property, on the outermost garment of clothing, on the front portion of the body, from the waist up.

The Gatepass System

The online Gatepass System allows the badged employees or contingent workers to:

- Request a pass for a known visitor
- Request a pass for person to be identified upon arrival (e.g., ride share services or deliveries)
- View the status of passes

If upon arrival at Argonne a visitor does not have a requested gate pass in the system, the host will be contacted for authorization.

The following passes require approval by a designated Division Approver:

- Passes that are requested for 5 days or greater
- Passes that are requested for night (7:00 p.m. - 6:30 a.m.), weekend, or holiday access

Note: Long term access will not be approved if the purpose of the visit can be accomplished with several shorter-term gate passes.

The Laboratory reserves the right to take appropriate disciplinary action for failure to adhere to all requirements for the admittance and hosting of visitors on site.

Laboratory Entrances and Gate Hours

Visit the Gate Hours web page for more information. Link to the site is provided on the last page of this document.

Hosting Foreign National Visitors

Approval must be obtained for all foreign nationals, 18 years of age or older, prior to accessing Department of Energy-owned or leased sites, information or technologies. To host a foreign national, you must:

- Be a DOE employee, Argonne employee or identified as an Argonne U.S. citizen contingent worker. **Note:** Employees from State Sponsor of Terrorism (SST) countries **cannot be a host**.
- Ensure the access is needed to support Department of Energy program objectives and/or US national interests
- Be current with SCD100: Foreign National Access Program Host Briefing
- Coordinate with your divisional FAVOR Administrative User/Representative to arrange for an ANL-593 to be submitted, and receive an approved ANL-593

Prior to access being granted, the appropriate immigration and naturalization documentation must be presented. Failure to provide the appropriate in-status documentation will result in a delay in gaining access.

Visit the Foreign National Access Program website link, on the last page of this document, for more information.

Scenario

You are going to conduct an employment interview through Skype with a Foreign National.

Do you need to have an approved ANL-593 - Foreign National Access Request Form before conducting the interview?

Yes!

Foreign Nationals must have an approved ANL-593 - Foreign National Access Request Form in the Foreign Assignment/Visit Request (FAVOR) system before the host can request a visitor pass in the Gatepass System, or before conducting employment interviews if specific Argonne or DOE business is going to be discussed - whether onsite or offsite, and regardless if it is in-person or virtual (e.g., phone, Skype, Blue Jeans).

NOTE: If the interview is only based on general conversation regarding the background of the foreign national, then no ANL-593 would be required.

VIP and Onsite Events Program

Program Mission
To provide a high level of service and ensure expeditious site access for Laboratory guests.

When hosting a VIP or an event on site, please contact the Security Logistics Coordinator to assist with site access planning and logistics of your event. (VIP Examples - DOE high-ranking official, Government officials, Laboratory Directors, Corporate Leaders, etc.)

You can submit a Vector request to register an onsite event. For your reference, link to the Vector page can be found on the last page of this document.

To contact Security for further information or questions, please reach out to us on our Hey Security! Teams Channel, or email us at heysecurity@anl.gov.

Thank you!

This concludes the SEC101, Counterintelligence, Classification, Export Control and Security Refresher Briefing.

For questions regarding the topics covered in this course and contact information, visit our websites.
For your reference, links to the websites can be found below.

Resources

- ANL-593 - Foreign National Access Request Form
  https://my.anl.gov/app/favor
- ANL-994 - Replacement of Lost Badge Form
  https://apps.inside.anl.gov/xink/displayForm.jsp?formNumber=ANL-994
- Classification Services Website (including Classification Analyst and Classification Officer)
  https://my.anl.gov/sas/service/classification-services
- Counterintelligence Website
  https://my.anl.gov/ci
- Counterintelligence Contact List
  https://my.anl.gov/ci/reference/counterintelligence-contacts
- Derivative Classifiers
  https://my.anl.gov/contact/r2a2-derivative-classifiers
- DOE O 470.4B, Safeguards and Security Program
  https://www.directives.doe.gov/
- Export Control Website
  https://my.anl.gov/bis/service/export-control
- Foreign National Access Program Website
  https://my.anl.gov/sas/service/foreign-national-access-program
- Gate Hours
  https://my.anl.gov/sas/reference/gate-hours
- Gatepass System
  https://my.anl.gov/app/gate-pass

- Hey Security! Teams Channel
  https://teams.microsoft.com/l/team/19%3ac6330acfb62f4596a41618d2bef350d6%40thread.tacv2/conversations?groupId=a05615b7-702c-48dc-9ace-fe6fa9320f0f&tenantId=0cfca185-25f7-49e3-8ae7-704d5326e285
- Information Security Website
  https://my.anl.gov/sas/service/information-security
- LMS-POL-6 – Traffic Safety
  https://my.anl.gov/esb/view/STELLENT/LMS-POL-6
- LMS-POL-19 - Protection of National Security and Other U.S. Interests
  https://my.anl.gov/esb/view/STELLENT/LMS-POL-19
- LMS-POL-23 - Export Control Policy
  https://my.anl.gov/esb/view/STELLENT/LMS-POL-23
- LMS-POL-67 - Visitor Site Access Approval
  https://my.anl.gov/esb/view/STELLENT/LMS-POL-67
- LMS-PROC-75 - Protecting Information in the Project Lifecycle
  https://my.anl.gov/esb/view/STELLENT/LMS-PROC-75
- LMS-PROC-105 - Strategic Partnership Projects Proposals
  https://my.anl.gov/esb/view/STELLENT/LMS-PROC-105
- LMS-PROC-320 - Hosting Visitors to Argonne
  https://my.anl.gov/esb/view/STELLENT/LMS-PROC-320
- Register an Onsite Event – Vector
  https://servicenow.anl.gov/sp?id=sc_cat_item&sys_id=8ac99f891b8d94901a84ddb6bc4bcbfc
- Security, Travel, and Emergency Services Website
  https://my.anl.gov/sas
- Site Access Manager
  https://my.anl.gov/sas/service/site-access
- Site Entry Requirements
  https://www.anl.gov/site-entry-requirements