2016

AT&T Global Business Public Sector Solutions

SECURITY: OUR SHARED RESPONSIBILITY

Table of Contents

Why Security is Important

Our commitment to security enables the protection of vital assets:

- People
- Customer sensitive and classified information
- Proprietary ideas and technology
- Facilities
- Critical infrastructure
- Mission activities
- AT&T business interest and reputation

All cleared affiliates are responsible for safeguarding information and material, the unauthorized disclosure of which might seriously impair or harm the interests of the Nation. Lack of adequate security may not only jeopardize the effectiveness of classified programs, plans and policies, but may result in the cancellation of contracts with Government agencies and the inability to bid on new contracts.

AT&T Global Business – Public Sector Solutions Security is here to help you fulfill that obligation. The objective of our security program is to ensure that all persons authorized to access classified information, or sensitive but unclassified information, know how to properly protect and handle the material, in order to prevent access by, or disclosure to, unauthorized individuals.

The Defense Security Service (DSS) oversees the protection of U.S. and foreign classified information and technologies in the hands of cleared industry under the National Industrial Security Program by providing professional risk management services. As Functional Manager for the Department of Defense (DoD), DSS provides security education, training, certification, and professional development for DoD and for 28 other U.S. Government agencies, their personnel and contractor employees. Public Sector Solutions Security works with DSS and our US government (USG) customers to ensure our security programs are compliant with all USG requirements.

Definitions

Public Trust

Government contracts sometime require hiring responsible people for judicious roles such as managing finances, overseeing processes, inspecting compliance, and protecting people and assets, among others. While many government contracting jobs do not require a security clearance, certain sensitive positions—often ones for protection of national security—demand especially knowledgeable and responsible employees. The USG designates such positions as “Public Trust Positions.” Approval for a Public Trust position does not authorize an individual to access Classified Information.

Classified Information

The term *classified* refers to information which our Government determines is vital to our national interest and for that reason, requires following Government-prescribed protective handling. There are three levels of classification: CONFIDENTIAL, SECRET, and TOP SECRET, which indicate sensitivity as follows:

- **CONFIDENTIAL** – Classified information, the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security that the original classification authority is able to identify or describe.
- **SECRET** – Classified information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
- **TOP SECRET** – Classified information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

CAUTION: The terms *TOP SECRET*, *SECRET*, and *CONFIDENTIAL* should only be used in connection with Government classified information.

Access

Access means the ability and opportunity to obtain knowledge of classified information. Access to classified information may be granted to persons who have both:

a. ***Eligibility***, also known as a Personnel Security Clearance (PCL) at least as high as the classification of the information involved. Public Sector Solutions Security must verify the security clearances for employees and/or visitors prior to access. A person’s word is NOT acceptable verification of clearance eligibility.

b. A ***need-to-know***, a determination made by the possessor of classified information that the prospective recipient has a requirement for access to, knowledge of, or possession of the classified information to perform tasks or services essential to fulfill a classified contract or program approved by a Government agency.

In simple terms: eligibility + need to know = access

Security Education

Indoctrination Briefing

Prior to permitting any employee or consultant to access classified information, the Facility Security Officer (FSO) or designated representative will brief the employee/consultant regarding the importance of classified information and his/her obligation for safeguarding it. The briefing will include the following:

a. A threat awareness briefing.

b. A defensive security briefing.

c. An overview of the security classification system.

d. Employee reporting obligations and requirements.

e. Security procedures and duties applicable to the employee's job.

Following the indoctrination, the employee/consultant will be required to sign the "Classified Information Nondisclosure Agreement" (NDA) and any other program specific documents required by the Government Cognizant Security Office (CSO).

Refresher Briefing

Every cleared employee shall receive a periodic refresher briefing, which as a minimum shall:

a. Reinforce the obligations discussed during the initial indoctrination briefing.

b. Inform employees of appropriate changes in security regulations resulting from recurring inspections that require corrective action or from changes in National policy.

c. As needed, provide instruction regarding the methods and operations used by hostile intelligence services to subvert U.S. industrial personnel and defensive measures to counter such subversion.

This document serves as your 2016 Refresher Briefing

Debriefing

A security debriefing will be administered to all cleared employees and consultants at the time of termination of employment (discharge, resignation, or retirement), when an employee's Personnel Security Clearance (PCL) is terminated, suspended, or revoked, or upon termination of the Facility Clearance (FCL). Debriefs will be administered when the individual no longer has a need to access classified information and is not otherwise supporting a classified contract.

Reporting Responsibilities

To comply with government reporting responsibilities, AT&T requires each cleared employee and those in the process of being cleared, to immediately report the following circumstances to Public Sectors Solutions Security:

- Suitability information. (See following topic)
- The loss, compromise, or suspected compromise of classified information.
- Efforts by an unauthorized person to obtain classified, or unclassified but sensitive information, (government, company, or private).
- Involvement as a representative in a foreign interest.
- Life changes such as birth or adoption of a child, marital status, co-habitation, home address, name change.
- Close and/or continuing associations with any foreign national.
- Any contact, even professional contact, with a representative of a foreign government.
- Unusual incidents or suspicious behavior that may occur during foreign travel.

Suitability Information Reporting

Suitability Information includes (but is not limited to):

- **Criminal Activities**
  –Any arrests - Any activity for which you could be arrested
  –DUIs, DWIs

- **Emotional or Mental Disorders, including treatment information** (Note: *treatment solely related to marital or grief counseling, or Post Traumatic Stress Disorder from combat related activities, need not be reported*)
  –All court ordered mental health treatments must be reported

- **Excessive Use of Intoxicants**
  –Refusal to accept rehabilitation assistance when offered
  –Failure to successfully complete rehabilitation when it is a mandatory condition for holding a clearance
  --Arrests related to intoxicant consumption (such as DUIs/DWIs, public intoxication)

- **Any involvement with illegal controlled substances or misuse of prescription medications**

- **Financial Issues**

  -- Gambling addiction or excessive gambling losses that impact financial solvency
  -- Garnishments
  -- Bankruptcy
  -- Foreclosures
  -- Unexplained affluence
  -- Identity theft

- **Security Violations**

  –Violations involving disregard of security regulations, whether intentional or inadvertent
  –Gross negligence in the handling of classified material
  –Violations indicating a pattern of negligence (repeated violations, even if minor)

Do not make Reports based solely on rumor or innuendo.

Counterintelligence (CI) Awareness

Counterintelligence (CI) is a proactive discipline intended to detect, assess, and deter threats from adversaries or insiders with the potential to cause loss of or damage to U.S. assets of value. *Threat* is defined as an adversary's intent and capability (evidenced by known doctrine, modus operandi, past successes, current activities, etc.) to exploit vulnerabilities in order to steal, compromise, or otherwise damage valued assets. External threats include, but are not limited to: foreign intelligence entities, terrorists, organized crime, hackers and cyber criminals. In addition to external threats, an *internal threat - the trusted "insider"* with authorized access – is a serious historic, current and projected concern relative to protecting U.S. assets. The insider actually represents both a threat and vulnerability: a trusted insider may act on his or her own to disclose sensitive information to unauthorized persons or otherwise harm protected assets; or may be exploited by external adversaries to compromise sensitive information or allow access to/damage other valued assets.

Protected Information

Intelligence collectors will often target a wide array of information in hopes of later "connecting the dots" to piece together a larger picture. While classified information is always highly coveted by our adversaries, corporate proprietary data can often be just as desirable. You must take care to properly safeguard all of the information you handle, including:

- Customer data (classified and unclassified)
- Employee data
- Vendor information
- Pricing strategies
- Proprietary processes
- Technical components and plans
- Corporate strategies and financial information
- Computer access protocols
- Business phone and email directories
- Passwords

Collection and Recruitment Tactics

Intelligence collectors use a variety of techniques to illicitly obtain our information. Some of those techniques include

- Elicitation: collection during seemingly innocent conversation
- Coercion or blackmail
- Appeals to ideology, disaffection with national or corporate policies or processes
- Financial enticement
- Electronic (listening devices, cyber intrusions, etc.)
- Social media or other open sources
- Recruitment of third parties (i.e. flight attendants, hotel &restaurant staff, etc.)
- Exploitation of joint ventures and/or research

For more information, please visit: http://www.dss.mil/documents/ci/CIAwareness.pdf

Insider Threats

Insider Threats include current or former employees, contractors, or business partners, with authorized access to company information, who misuse that information for their own benefit or that of a competitor or foreign nation. Possible motivations can include the need or desire for money, conflicting ideologies or disaffected political sympathies, psychological factors such as exaggerated desire for adventure/excitement, ego gratification, and misplaced anger.

Research by the *CERT Insider Threat Center* indicates that insider bad actors typically conduct their attacks within 30 days of giving their resignation and often display certain behavior prior to their illicit activities, such as threatening the organization or bragging about how much damage they could do.

Behavior that might indicate a potential insider threat includes:

- Attempts to expand access beyond job requirements
- Sudden reversal of financial situation
- Outward disgruntlement towards employer
- Paranoia that they are under investigation
- Working odd hours inconsistent with job assignment
- Unreported foreign contacts or foreign travel when required to report
- History of security infractions or indifference to policies

For more information, please visit: http://www.dss.mil/documents/ci/InsiderThreat.pdf

Employee Countermeasures

We are the first line of defense in safeguarding both company proprietary and USG classified information. Some simple ways to lower your risk of being targeted by an adversary and better fulfill your responsibilities as a cleared employee include:

- Maintain a responsible and professional social networking presence.
- Avoid identifying yourself as a cleared employee on social or professional networking sites.
- Always utilize Voltage encryption when sending sensitive email communications.
- Follow all company and customer IT policies and procedures.
- Never discuss sensitive information in public places; that includes public areas within our own facilities.
- Don’t respond to or open questionable electronic communications.
- Always maintain a keen awareness of surroundings and notify Public Sector Solutions Security of any anomalies or concerns.

If you See something, Say something. When in Doubt, Report it!

Social Media Vulnerabilities

Social media sites are used extensively by our adversaries to collect information. If you choose to use social media sites, assume that anyone can see anything you post and follow these guidelines:

- Only accept or maintain connections with people you know.
- Ignore requests to “friend” or “link” from strangers.
- Ensure that family members take similar precautions.
- Don’t post smartphone photos (which can be geo-tagged).
- Set privacy and sharing options to be most restrictive.
- Don’t post work details, contacts, locations, or name government customers.
- Don’t post travel plans whether personal or business related.
- The fact that you hold a security clearance or a public trust position is **NOT** appropriate information for any social media site.

The U. S. Navy has created some good social media guidelines:

Facebook: http://www.public.navy.mil/usff/Documents/FaceBook%20Smart%20Card.pdf
Google+: http://www.public.navy.mil/usff/Documents/Google+%20Smart%20Card.pdf
LinkedIn: http://www.public.navy.mil/usff/Documents/LinkedIn%20Smart%20Card.pdf
Twitter: http://www.public.navy.mil/usff/Documents/Twitter%20Smart%20Card.pdf

For more information about social media and social networking, please visit: http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks

Social Engineering

A social engineer tries to collect information from one or more sources to gain access to protected information. Social engineers exploit the weakest link in our security: people. No reputable organization will ever call or email you to ask for a user name, password or other credentials. Be wary of unsolicited phone calls or email from anyone claiming to want to “help” you or the company or those requesting company contact information or other information that an employee, customer, or partner should be able to readily access on their own. If contacted by a new employee that you do not know, confirm their identity and role before sharing any information. If the contact seems strange, report it to Security.

Trust, but Verify!

Cyber Security

The same threats to our facilities, personnel, and information also apply to our networks and devices. Thanks to our increasingly connected world, an adversary no longer needs access to our physical facilities; they can steal information or launch an attack from thousands of miles away. Hackers use several tools to gain access to and compromise a system or network:

- Email with malicious links or attachments
- Un-patched or outdated software vulnerabilities
- Removable media (USB drives)
- Use of weak or default passwords
- Website vulnerabilities
- Attacks against PKI credentials (i.e., stolen logon credentials)
- Spoofing emails that imitate valid sender addresses and domains

Most attacks start with “phishing” Email that includes a malicious link or attachment. If a well-intentioned but careless insider clicks that link or opens the attachment, malware can be introduced that gives the attacker access to their device or system. It is estimated that as many as 95 percent of successful hack attacks or incidents are attributed to human error.

Cybersecurity Tips

- Use a complex alpha-numeric password with a combination of numbers, symbols, and upper/lower case letters (most systems require this)
- Change your passwords regularly
- Do NOT open emails or attachments from unfamiliar sources, even if they look official unless/until you verify authenticity
- Do NOT install or connect any personal software or hardware to your organization’s network or hardware without permission from IT Services or your ISSM/ISSO
- Report all suspicious or unusual problems with your computer to your IT Services or CSO. In the case of a classified system, notify your FSO or ISSM.

Don’t Delay, Call Right Away!

For more information, visit the Chief Security Office (CSO) web site at: http://cso.att.com/

Classified Visits

- **Incoming**
  Visitors who require access to classified information must have a current visit request and clearance certification on file with the specific Public Sector Solutions Security Office.
- **Outgoing**
  All classified visits must be coordinated with your Public Sector Solutions Security Office. If you are planning a classified visit to another company, military installation, or Government agency, you should discuss and verify your proposed visit with your point of contact before notifying and requesting that your Public Sector Solutions Security Officer initiate the visit clearance action.

Storage

Classified material must be stored in an approved security container provided by Public Sector Solutions Security. Classified material must be under the control of properly cleared personnel at all times when it is not secured in an approved container.
Public Sector Security strongly recommends that every AT&T cleared facility that stores classified information implements a system of security checks at the close of each working day to ensure the secure disposition of all classified material and security containers.

Safes and Combinations

All requests for safes shall be coordinated with Public Sector Security. Security personnel are responsible for changing all lock combinations, maintaining associated records, and procuring all repair services with respect to safes, dials, and applicable locks.

The number of individuals given a combination will be limited to the minimum required to operate efficiently. Safe combinations will be provided only to those persons who have a bona fide need for the information stored in the container. Individuals entrusted with combinations must have a clearance that meets or exceeds the highest level of classified information stored in the container. When an individual possessing a combination transfers organizations or terminates employment, the employee shall notify the respective Security Office.

Records containing safe combinations will carry the same level of classification as the material stored in the container. Combinations to security containers must be committed to memory.

Transmitting Classified Information

Maintaining control and accountability of classified information is a critical responsibility. Always consult with your FSO, your CSSO, or the Public Sector Solutions Security office for specific guidance before transmitting classified information. Some general rules follow:

Within Facility

A formal transfer of custody is not required when a cleared person loans a classified document to another appropriately cleared person in the same building on a temporary "need-to-know" basis. However, for your protection, you should record the transaction. Remember, if you loan a document and fail to get it back, it is your responsibility.

Outside Facility

There are very strict government rules and AT&T procedures regarding hand carrying classified information. Classified information must be properly wrapped and transported, and a courier briefing must be provided by either your FSO or your government customer. If possible, it is preferable to electronically transmit classified information rather than transporting hard copy documents. Always ensure that the IT system is classified and accredited at the level of the information or higher. If you have questions, contact Public Sector Solutions Security.

Hand Carrying on Travel

Hand Carrying classified information while traveling constitutes a serious risk and should be avoided. Whenever possible, transmit material to your destination electronically using appropriate classified systems. If not possible to use IT systems, some material may be mailed, depending on the level of classification. The Defense Courier System is also an option in some circumstances. If there is no alternative to hand carrying, employees must receive a courier briefing from Security. The individual must retain the material in their personal possession while en route to the destination. Classified material cannot be stored in hotel rooms, hotel safes, baggage, lockers, automobiles, or private residences. The courier must deliver the material directly to an authorized cleared facility upon arriving at the destination on the same day of travel and a receipt must be signed and returned to AT&T's Security Office. Overnight storage can only occur at approved facilities.

Creating Classified Material

The type of work performed within the Company periodically necessitates the origination or production of classified work materials in various forms, from working papers to completed final publications. All such material shall be accountable and produced on classified systems only. Contact your security office for guidance BEFORE creating classified or potentially classified materials.

AT&T cleared personnel who create, edit, or derivatively classify material, must first complete *Derivative Classification* training as set forth in NISPOM paragraph 4-102 and at least once every 2 years thereafter. For more information, see: http://www.cdse.edu/documents/cdse/DerivativeClassification.pdf

Marking

Proper Security Classification Markings shall be applied when generating or copying classified material. In addition to headers and footers which provide the overall classification of the document, the title and each paragraph or portion of the document must be properly marked at the beginning with: (U) for unclassified, (C) for confidential, (S) for secret, or (TS) for Top Secret and any handling caveats (e.g., NOFORN, ORCON, etc). It is strongly recommended to use unclassified titles so that the receipt describing the document can be an unclassified document. The “Classified By” Line shall include the company name and, when applicable, the division or branch, followed by the name and position or personal identifier of the derivative classifier.

Classification Guidance

Government contracts involving access to classified information include specific security requirements and guidance in the “Contract Security Classification Specification” (DD Form 254). Prior to generating new material, originators must review the DD Form 254 and any Classification Guides referenced therein. Program Management or Security can provide you with this information.

Reproduction

Please consult with your FSO, CSSO or the Public Sector Solutions Security Office before reproducing classified material.

Destruction

Classified documents must be destroyed in an approved shredder. If you have questions, contact your FSO. The Security Office must securely destroy all classified material other than documents. Contact your security office for secure equipment destruction procedures.

Retention

Contractors may retain classified material received or generated under a contract for a period of two years after completion of the contract, provided the applicable Government Contracting Activity (GCA) does not advise to the contrary. The GCA shall provide written authorization for additional retention or transfer of the material to a current applicable contract.

Classified Information System (IS) Security

Each program that uses a computer system to process or store classified information shall have a designated Information System Security Manager (ISSM) in addition to a Facility Security Officer (FSO). The ISSM and FSO shall obtain USG/CAS approval and accreditation BEFORE processing any classified information on a computer system. The ISSM will brief personnel requiring access to classified computer systems on their responsibilities.

All users shall:

a. Comply with the IS Security Program requirements.
b. Be aware of and knowledgeable about their responsibilities in regard to IS security.
c. Be accountable for their actions on an IS.
d. Ensure any authentication mechanisms (including passwords) issued for the control of their access to an IS are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.
e. Receive an IS briefing and acknowledge, in writing, their responsibilities for the protection of the IS and classified information in compliance with the Company's "Information System Security Plan".

Physical security safeguards shall be active at all times to protect the hardware and software integrity of the Automated Information System (AIS), including remote equipment, even when the AIS is not processing or storing classified information. Protection is commensurate with the classification level and category of the information, the threat, and the operational requirements associated with the environment of the AIS.

Foreign Travel

Personnel with access to classified material shall report all foreign travel and visits to foreign embassies at **least 30 days** in advance to the Public Sector Solutions Security Office. Travel and Briefing forms are available from your security officer as well as on the Public Sector Solutions Security website at http://gov.web.att.com/departments/security/forms.asp Some SCI and SAP sponsors may have slightly different reporting requirements. Be sure to contact your FSO to obtain the correct forms

Foreign Travel Safety

Whether traveling on personal or company business, a cleared person is always a potential target when in a foreign country where foreign intelligence services have better access to you and their actions are not restricted by US law.

For your personal safety, Security recommends use of the State Department Smart Traveler Enrollment Program (STEP) for all foreign travel. Visit: http://step.state.gov

Unless traveling on classified business (not common), there is no reason for anyone to know you have a security clearance. Don't advertise it! It's also common to be targeted simply as an employee of AT&T since industrial espionage is alive and well in many foreign countries. Keep in mind that both industrial and government spies are frequent visitors to conferences and trade shows. The Defense Security Service (DSS) recommends:

- Do not publicize travel plans and limit sharing of this information to people who need to know.
- Do not post pictures or mention you are on travel on social media until your return
- Attend pre-travel security briefings.
- Maintain control of sensitive information, media, and equipment. Pack them in your carry-on luggage and maintain control of them at all times. Do not leave them unattended in hotel rooms or stored in hotel safes.
- Keep hotel room doors locked. Note how the room looks when you leave compared to when you return.
- Limit sensitive discussions; public areas are rarely suitable for discussion of sensitive information.
- Do not use computers or fax equipment at foreign hotels or business centers for sensitive matters.
- Ignore or deflect intrusive or suspicious inquiries or conversations about professional or personal matters.
- Keep unwanted sensitive material until it can be disposed of securely.
- Attend post-travel debriefing.

Avoid bringing company issued laptops or devices unless necessary since they too are targets. If bringing a device, including a smart phone, keep it under your control at all times. DSS recommends these steps to protect information and devices:

- Leave unneeded electronic devices at home.
- Use designated travel laptops that contain no sensitive or exploitable information.
- Use temporary email addresses not associated with the company.
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return.
- Encrypt data, hard drives, and storage devices whenever possible.
- Use complex passwords.
- Enable login credentials on laptops and devices.

For more information, please visit:
http://www.dss.mil/documents/ci/ForeignTravelVulnerability.pdf

Meetings, Seminars, and Conferences

Coordination with Public Sector Solutions Security shall occur as far in advance as possible, regarding planned classified meetings. Security personnel will assist in maintaining necessary security and control of classified material used or distributed at the meeting. The meeting host will appoint a monitor for each classified meeting to assure compliance with security regulations. Required for all classified meetings:

- Attendee Verification: Employees and visitors must have an appropriate security clearance and an established need-to-know for the classified information to be presented at Company sponsored or hosted conferences, seminars, or meetings. The security clearance of each individual (employees and guests) invited to a meeting must be verified by Public Sector Security prior to admission.

- Security Classification of Meeting: The speaker or monitor will announce the classification to the audience at the beginning and end of each presentation.

- Classified Material Distribution: The monitor must keep a record of distribution of classified material and must account for all classified material at the conclusion of the meeting.

- Note taking: The monitor will collect any classified notes at the end of the meeting and take them to the Security Office for control, outside transmittal, or destruction, as applicable.

- Area Inspection: The monitor shall scan the room/area during breaks and inspect the room at the conclusion of the meeting, to ensure that there is no classified information left unattended within the room.

Dissemination and Public Disclosure

Need-to-know and appropriate clearances are essential prerequisites for discussion of classified information with members of the Government, industry, and fellow employees. One without the other is not enough. No person is entitled to access classified information solely by virtue of his/her rank or position. Should there be any question regarding the clearance status of an individual, contact Public Sector Solutions Security.

Contractors shall not disclose classified or unclassified information pertaining to a classified contract, without prior review and clearance as specified in the “Contract Security Classification Specification” (DD Form 254) for the contract.

Our Shared Responsibility

Protecting classified and proprietary information depends, today more than ever, on YOUR security awareness. YOU can literally make or break any AT&T or customer security program.

In today's Information Age, when an employee can inadvertently disclose secrets or spread malware with just the click of a mouse, the stakes are higher than ever. Today's threat-driven environment increasingly plays host to a growing number of security risks from criminal hackers, terrorists, foreign intelligence services, industrial spies and information/identity thieves. So, how do we ensure that government and corporate secrets are protected? To quote a popular CSO campaign, ***" You are the firewall".*** Employee awareness, an essential element in any successful security program, remains our first line of defense.

The Public Sector Solutions Security Team

The Public Sector Solutions security team plays a vital role in educating employees on their responsibility to protect AT&T's and the government's information. The security team addresses everyday threats and vulnerabilities to information and practical ways to counter them. AT&T is committed to its security program and encourages employees to take part. It also provides proof-positive evidence to government security inspectors that our company takes its security responsibilities seriously.

All cleared AT&T employees have a Security Administrator or Team supporting their classified activities and holding their security records. If you are physically located at an AT&T facility, contractor, or Government site, this support may not always be apparent to you. If you have any questions about which AT&T facility actually supports your clearance and holds your security records, call the AT&T Vienna, VA facility at either of the following numbers:

703-506-5707 or 703-506-5704

SECURITY INTRANET WEBSITE:

http://gov.web.att.com/departments/security

Remember, Security is OUR Shared Responsibility

ACKNOWLEDGEMENT FOR SECURITY REBRIEF 2016

I acknowledge that I have received the Security Rebrief 2016, which contains the following information:

- Importance of Industrial Security
- An overview of the security classification system
- Security Education
- Reporting Responsibilities
- Counterintelligence Awareness
- Social Media
- Social Engineering
- Cyber Security Awareness
- Classified Visits
- Creating, Transmitting and Storing Classified Information
- Classified Information System Security
- Foreign Travel
- The Public Sector Solutions Security Team

________________________________/_________________________________

Print Name Signature

________________________________/_________________________________

Date ATTUID Number

________________________________/_________________________________

Primary Work Location Immediate Supervisor