DTRA Security and Counterintelligence In Processing

Detect. Deter. Defeat.

Unclassified

Initial Security and Counterintelligence Briefing

Your assignment to, or employment by, the Defense Threat Reduction DTRA (DTRA) carries responsibilities for safeguarding all classified and sensitive unclassified information you may come in contact with. You are responsible for helping maintain DTRA's security posture and complying with applicable policies. Failure to comply with the security procedures outlined within is reportable to the DoD Consolidated Adjudications Facility (CAF). Your responsibilities are covered in this briefing:

- **ADMINISTRATIVE INFORMATION**

- **DTRA BADGE AND CAC POLICY**

- **SAFEGUARD SENSITIVE AND CLASSIFIED MATERIAL**

- **NATO/CNWDI/RD PROGRAMS**

- **MANDATORY REPORTING REQUIREMENTS/SECURITY INFRACTIONS OR VIOLATIONS/PERSONAL BEHAVIOR**

- **INSIDER THREAT**

- **PROHIBITED ENTRY ITEMS**

- **COMMUNICATIONS SECURITY (COMSEC)/OPERATIONS SECURITY (OPSEC)**

- **ACCESS TO CLASSIFIED INFORMATION**

- **SECURITY IN/OUT PROCESSING**

Administrative Information

MANDATORY WHEN YOU ARRIVE OR DEPART DTRA

IN/OUT PROCESSING
Check out in/out processing on the DTRANet!
703-767-1278
Sc_in/outprocessing@dtra.mil
DTRA Security & Counterintelligence Office
"Professionalism, Teamwork, Customer Service"

- Review all information and ensure you understand before signing or accepting.

- All forms, brochures, contact numbers and addresses mentioned in this briefing may be obtained upon request. If you need further information or clarification, please ask your Security Representative.

- If your duty location is off-site, your local Security Representative will provide site-specific information, such as evacuation locations, burn run schedule, etc.

- Cyber Awareness Challenge & PII training are required prior to gaining access to DTRA Local Area Networks (LAN). Print a copy of the completion certificates, and email them to your servicing Security Office with the subject line "In- Processing Paperwork".

- DTRA Policy REQUIRES you to out-process DTRA upon PCS, completion of assignment or contract, retirement, etc. You must return all DTRA-issued items (badge, CAC, SNET token) to the Personnel Security Office. DO NOT give these items to your supervisor, sponsor, COR, etc. You must bring them to the Personnel Security Office and officially out process. Failure to out-process is a reportable security concern and may delay or prevent in-processing with Security at your next duty assignment.
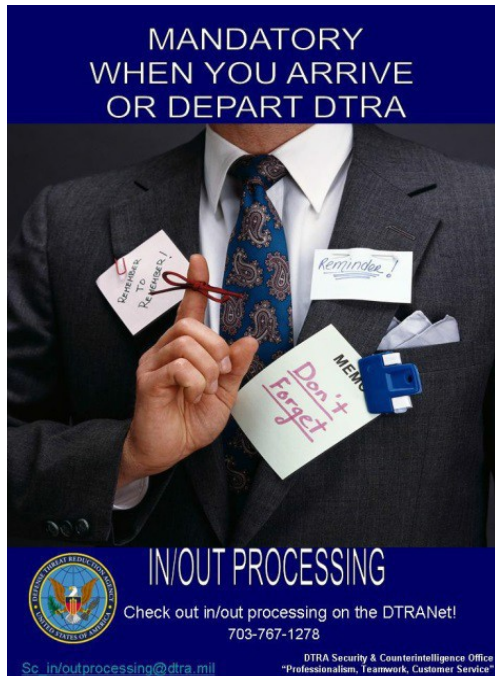
DTRA Badge & CAC Policy

DTRA-issued Badges are automatically disabled after 90 days of non-use. LAN accounts are automatically disabled after 30 days of non-use, and are deprovisioned after 45 days. More than two instances of disabling due to non-use will require a justification from your DTRA Sponsor/PM/COR in order to be reactivated!

WEAR the DTRA badge face-forward, above the waist, and on their outermost garment at all times within or between buildings. Never allow other personnel to use your DTRA badge for any reason; do not allow other personnel to follow you through a check point/turnstile without badging themselves in or out.

CHALLENGE any individual within DTRA facilities who are not wearing a DTRA badge. Escort any individual within a DTRA facility who is not wearing a DTRA badge, or unescorted individuals wearing a red ESCORT REQUIRED badge to Access Control.

REMOVE when not inside a DTRA facility or enclosed/fenced-in area. You are accountable for your badge at all times. To avoid theft, do not leave badge unattended in your vehicle.

REPORT lost or stolen issued IDs (badge/CAC/courier) in writing immediately to your site/field Security Office.

PROGRAMMING of badge to special exclusion areas – Contact your local Security Manager for coordination.

RETURN all DTRA-sponsored badges and IDs issued to you when Out Processing.

NEVER use your DTRA badge as a form of ID outside of DTRA facilities.

Common Access Card (CAC)

What is the purpose of a CAC?

✓ DoD Identification for access onto Military Bases

✓ Access to DoD Information Technology Systems

Important: You will create a PIN at time of CAC issue. This PIN is used for LAN access. **Be sure to remember your PIN!**

How Do I Get My CAC? CONTRACTORS ONLY

- Personnel Security will provide you with the TASS application for a DTRA-sponsored CAC card upon receipt of your DTRA Form 3 from your sponsor.

- TIPS
    - New password must be *EXACTLY 14* characters. We recommend you use your temporary password, but change the last character. You will not need to remember or use this password again. Provide the TASS temporary login and password sheet to Personnel Security for destruction upon completion.
    - *DISREGARD* warnings about your email address and contract number

- After you submit the application, your Trusted Agent will review and approve the application on your scheduled in-processing date/time. Next you will proceed to any RAPIDS location https://idco.dmdc.osd.mil/idco/. If on site at DTRC, you can go to the DLA CAC office. You will need to take two forms of federal, state or local government identification containing a photograph or information containing name, date of birth, gender, height, eye color and address.

- Personnel Security will request your UNET account when you in process.

- Take your CAC to the DTRA Help Desk to have DTRA certificates loaded and your .mil email address provisioned.

Important: Everyone *MUST Out-process with DTRA Personnel Security* and return *ALL* DTRA Issued items. (CAC, DTRA Badges, NCR/Pentagon Badges, Courier Cards and SNET tokens)

How Do I Get My CAC? CIVILIANS ONLY

- **Civilians**: DTRA HR will provide you with an appointment time and date for CAC issuance.
  - Bring the CAC to the DTRA Help Desk to have certificates loaded onto the CAC

COMMON ACCESS CARD (CAC)
DOCUMENTS
THAT ESTABLISH IDENTITY

AUTHORIZED ID'S used to obtain a CAC card (NOT EXPIRED):

01	Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address
02	ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address
03	School ID card with a photograph
04	Voter's registration card
05	U.S. Military card or draft record
06	Military dependent's ID card

NOTE: Name Changes - New Driver's   **The DTRA Badge is NOT an authorized form of ID**

- **Military**: Once your UNET has been created (normally 24 hours after in-processing), proceed to the DTRA Help Desk to have certificates loaded onto your CAC.

Safeguard Sensitive and Classified Material

Each individual assigned to DTRA is responsible and accountable for handling classified information/material to prevent its unauthorized disclosure. When removing classified information from approved storage and safekeeping, attach the appropriate cover sheet. The following three cover sheets are placed on top of documents to clearly identify the classification level of the document and protect classified information from inadvertent disclosure.

Classified materials must be destroyed when no longer required to maintain. Classified documents that are no longer needed will be placed in burn bags and destroyed during the weekly burn run or by an NSA approved cross-cut shredder. If you are not assigned to the DTRC, check with your Field Office for local procedures.

Classified CDs and floppy diskettes may be destroyed by incineration. Classified CDs may also be destroyed through the use of a device that has been identified on the National Security DTRA Evaluated Product list of the Destruction of Optical Media.

NATO/CNWDI/RD Briefings

*If you require access to the SNET, you are required to receive the NATO briefing.

➢ **NATO** (COMPLETE DTRA Form 22)

The NATO program is governed by the United States implementation of NATO security procedures (USSAN Instruction 1-70) All personnel with access to NATO confidential and higher require a formal NATO briefing. All NATO material will be stored separately from U.S. Classified materials. The registry will control and bring under the DTRA NATO accountability system all NATO secret and above material. The registry will maintain document receipts and files for NATO secret and above material. All NATO transactions for NATO secret and above will be processed through the NATO registry (no exceptions).

➢ **RD/FRD/CNWDI** (COMPLETE DTRA Form 21)

If your assignment at DTRA requires you to have access to Restricted Data (RD), Formerly Restricted Data (FRD), and/or Critical Nuclear Weapon Design Information (CNWDI), you are required to become familiar with the procedures for identifying, classifying, marking, handling, and declassifying documents containing that information as required by the Atomic Energy Act and 10 CFR Part 1045.

MANDATORY Reportable Items

Significant personnel security issues _may_ result in suspension of access or revocation of security clearance. Below is a list of items that you MUST report in writing to Personnel Security or your local Security Specialist. When in doubt, report – don't take any chances.

Foreign Travel/Foreign Contact/Foreign Activities

Attempted Elicitation

Misuse of government property or IT systems

Media Contacts

Marital Status

Criminal Conduct

Financial Anomalies

Alcohol and Drug-related treatment

Mental Health

Reportable Actions by Others

Make the right choice – Just report it!
Please read the brochure carefully.

MANDATORY Reportable Items, Continued…

Foreign Travel:

- Report unofficial foreign travel as soon as you are aware of the upcoming travel. Refer to the Reporting Requirements quick link on the DTRA1 for reporting procedures and forms.

- DTRA encourages you to report official travel to the Briefing/Debriefing Center.

- Schedule a CI Foreign Travel Briefing (via email) with the Briefing/Debriefing Center. Unanticipated border crossings into any foreign country not included in the traveler's approved itinerary, regardless of duration, are discouraged. All deviations from travel itineraries shall be reported within five business days of return.

- Schedule your Foreign Travel debriefing (via email) within 10 business days of your return.

Foreign Contact:

- Report all foreign contact. Refer to the Reporting Requirements quick link on the DTRA1 for reporting procedures and forms.

- Report contacts with a known or suspected foreign intelligence entity, as well as continuing association with known foreign nationals that involve bonds of affections, personal obligation, or intimate contact; this includes roommates, an foreign national who co-occupies a residence for a period exceeding 30 calendar days, or contact that involves the exchange of personal information.

- Schedule a CI threat briefing 30 days prior to expected official contact with foreign nationals within the U.S.

Foreign Activities:

Report application for and receipt of foreign citizenship; application for, possession, or use of a foreign passport or identity card for travel; involvement in a foreign business or organization (to include employment and volunteering), foreign bank account, foreign property, voting in a foreign election, or adoption of a non-U.S. citizen.

Make the right choice – Just report it!

MANDATORY Reportable Items, Continued…

Attempted Elicitation:

Report any actual or attempted exploitations, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of the means used.

Misuse of Government Property or IT Systems:

Report any actual or suspected **u**nauthorized access or use of IT systems. Viewing, transmitting, or soliciting sexually oriented material or images; transmitting profane, obscene, abusive, offensive, or harassing statements is strictly prohibited. (see DTRA FM 205 for further information)

Media Contacts:

Any release of DTRA information, to the media or otherwise, must be approved through the DTRA Public Affairs Office. You must report any other contact with or solicitation from the media even if the contact does not result in an unauthorized disclosure. If any member of the media contacts you for information, refer them to Public Affairs; never comment on news releases pertaining to DTRA or classified information.

Change in Marital Status

Reportable changes in status include marriage, intent to marry, legal separation, divorce, and cohabitation that involves living with and sharing bonds of affection, obligation or other commitment

Know the Facts…

Use of Marijuana and the Effect on a Security Clearance Eligibility

Any drug use which is illegal under federal law can detrimentally affect your eligibility to hold a security clearance.

- Use and/or possessing marijuana is still a federal crime
- On the SF86 Security Questionnaire Section #23 In the last seven (7) years, have you illegally used any drugs or controlled substances and your response is "Yes"
  - You will be flagged as having engaged in criminal conduct
  - Bad news is your background now reflects derogatory information

Medicinal Marijuana Use
- Medicinal marijuana use has not been legalized under federal law

NO PORN!

Self Reporting

Need Help? Come See Us!

Self Reporting is essential in maintaining the integrity of the Personnel Security Program. If it is discovered that an employee concealed relevant information during the investigation or after the clearance was issued, their clearance can be revoked. All employees who occupy a sensitive position and/or have access to classified information are expected to self report changes or incidents that may impact their clearances. Self reporting, while mandatory, is also a question of personal integrity and certainly preferable to the incident or change being discovered.

Misuse of Information Technology Systems
(Is one example of item to be self reported)

For more information please contact Personnel Security

Make the right choice – Just report it!

Mandatory Reportable Items, Continued…

Reportable Actions by Others:

Your obligation to protect national security includes reporting any of the above behaviors known or observed in other cleared personnel, as well as any unwillingness to comply with rules and regulations or to cooperate with security requirements, unexplained affluence or excessive indebtedness, alcohol abuse, illegal drug use/activity, criminal conduct, misuse of government property or IT systems, mental health issues where there is reason to believe it may impact the individual's ability to protect classified or sensitive information, and any activity that raises doubts as to whether the individual's continued clearance eligibility is clearly consistent with the interests of national security.

Security Executive Agent Directive 3
When should I report: ASAP

Report information as soon as you plan, become involved in or prior to participation in an activity.

If unable to report immediately, you should report to Personnel Security within 24 hours of an event.

Make the right choice – Just report it!

Security Infractions and Personal Behavior

REPORT ALL SECURITY INFRACTIONS AND VIOLATIONS

Immediately report all security violations, security infractions, or practices dangerous to security to your Security Manager and to DTRA Security personnel.

PERSONAL BEHAVIOR

You must exercise vigilance, caution, and discretion in your personal conduct to avoid being placed in compromising situations.

Be wary of anyone attempting to befriend you for no obvious reason or involve you in a romantic escapade. Such tactics have frequently been employed by foreign intelligence services.

Insider Threat

- Insider threats exist in DTRA and it is everyone's responsibility to help safeguard our information, facilities, and personnel

- Not all insider threats are intentional! A great deal of technology and information is lost because of carelessness

- Report anything of concern; our team will direct to the appropriate office

Reportable Indicators

Reportable indicators of suspicious behaviors include, but are not limited to:

- Attempting to expand access for duties beyond normal responsibilities

- Displaying questionable loyalty to US government

- Performing repeated or unrequired work outside of normal duty hours

- Exhibiting behavior that results in repeated security violations

- Engaging in illegal activity or asking you to engage in any illegal activity

- Attempting to elicit personnel with access into compromising situations

- Changes in financial circumstances:

    - Displaying unexplained or undue affluence

    - Sudden repayment of debts, bragging of money

- Exhibits actions or behaviors associated with disgruntled employees:

    - Conflicts with supervisors and coworkers

    - Decline in work performance

    - Tardiness

    - Unexplained absenteeism

INSIDER THREAT PROGRAM (PP-SCC)

IT NEVER PAYS TO BE AN INSIDER

WANTED   12 Years $20 Mil   KILLED   DEATH PENALTY
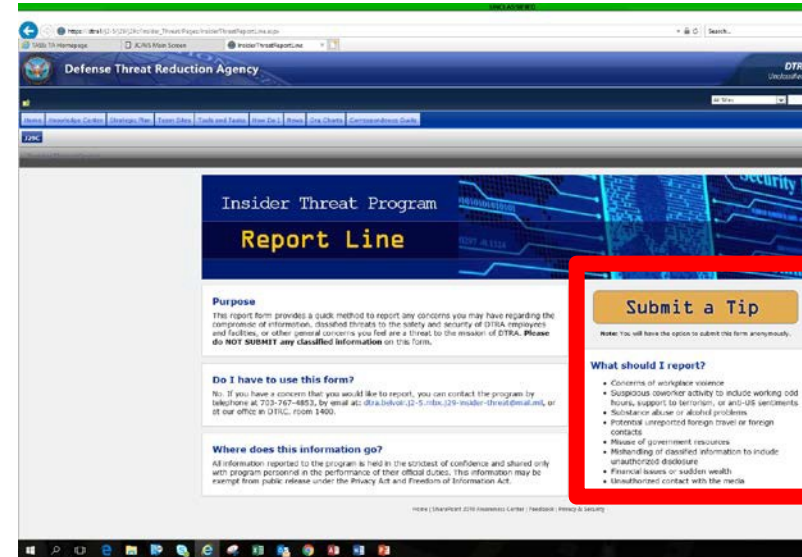
Why Co-Workers Might Not Report

- Didn't consider the activity important enough to take action
- Didn't recognize observed behavior as suspicious or a threat
- Didn't want to be identified as a "tattler"
- Didn't know how to report the suspicious behavior

How Employees Can Contact Us

When reporting on the tip line on DTRA1, you can choose to remain anonymous

Contact Us:

Email: dtra.belvoir.oi.list.oi-msc-insider-threat-tm-govt@mail.mil

DTRA1 Portal: https://dtra1portal.unet.dtra.mil/OI/MS/Insider_Threat/default.aspx

Room: 1400

Telephone: (571) 616-6123 or (703) 767-4853

Prohibited Entry Items

Cameras, weapons, wireless devices, smart watches, and other portable electronic devices are not permitted within DTRA spaces without express written permission or waiver. Prohibited electronic devices include both personal and government- issued devices, to include smartphones, e-readers, tablets, laptops, unapproved smart watches and similar devices. DTRA UNET laptops and approved medical devices are exempt from this policy. Certain personal wearable fitness devices are permitted when they appear on the approved devices list; however, connecting to DTRA systems or networks is prohibited. DTRA may conduct random searches at any time to confirm policy compliance. Wireless detection equipment will be used to monitor compliance with this policy

No electronic devices, personally or government owned, are permitted in any DTRASCIF *without written* approval from the Special Security Officer (SSO).

Wireless devices are prohibited for use within all DTRA facilities.

Personnel who do not wish to leave their wireless device in their vehicles, may store them in the lockers provided in the main lobby of the DTRC or similar storage lockers at other DTRA facilities. Wireless devices must be turned off prior to entering DTRA facilities and placed in the locker. These lockers are provided as a courtesy for day-use only; do not take the key to the locker home with you.

Unauthorized Disclosure

Discuss classified information only with those who have the appropriate security clearance and a valid need-to-know. Verification of need-to-know rests with the person who controls the information. When in doubt, do not divulge information. Remind recipients of the classification of the information you are about to discuss. Do not comment on any news releases pertaining to DTRA.

If contacted by the media or general public, refer the caller to Public Affairs, 703-767-5870.

If contacted by the media outside of normal duty hours, refer the caller to 703-767-2003, who will notify Public Affairs.

Please do not comment.

COMSEC and OPSEC Awareness

COMMUNICATIONS SECURITY (COMSEC) AWARENESS

Use of the duty phone constitutes consent to COMSEC monitoring. Never discuss classified information over standard duty phones and do not attempt to "talkaround" classified information. Use your HOLD button when calling someone else to the phone or when assisting a customer. Do not fax classified material using an unclassified fax machine and do not use a fax machine as a copier.

OPERATIONS SECURITY (OPSEC) AWARENESS

While we have traditional methods to protect classified information, we also deal with unclassified but sensitive information that, if revealed, could expose areas where DTRA could be vulnerable. Be familiar with sensitive unclassified information and be aware of to whom you reveal this information. If in doubt, do not reveal it.

No office paper, regardless of classification and/or sensitivity will be disposed of in a trash basket, garbage can, dumpster or recycle bin. All office paper will be placed in a burn bag for centralized destruction or shredded. Office paper is defined as paper items containing either computer-generated or hand-written print; this includes, but is not limited to printer paper, notebook paper, post-its, scratch pads, calendar sheets, etc.

Security Clearance

A security clearance is a privilege, not aright.

When you accept the privilege of having access to classified and sensitive information, you also accept the responsibilities that accompany this privilege.

This is a lifelong responsibility.

Access to Classified Information

Requirements for Access to Classified Information:

As an employee of the U.S. Federal Government or one of its contractors, licensees, or grantees in a position that requires access to classified information, you must:

1. **Possess a valid Security Clearance (Eligibility)**

    You have been the subject of a personnel security investigation to determine your trustworthiness for access to classified information. As an individual who has been granted a security clearance (eligibility), you have met the first of three requirements necessary to have access to classified information.

Access to Classified Information

Requirements for Access to Classified Information:

1. Possess a valid Security Clearance

2. **Have an official "Need-to-Know"**

    The holder of classified information determines Need to Know.

    Need to Know is based on a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program in the interest of national security.

    Access to classified information shall not be afforded to any individual solely by virtue of office, position, or security clearance.

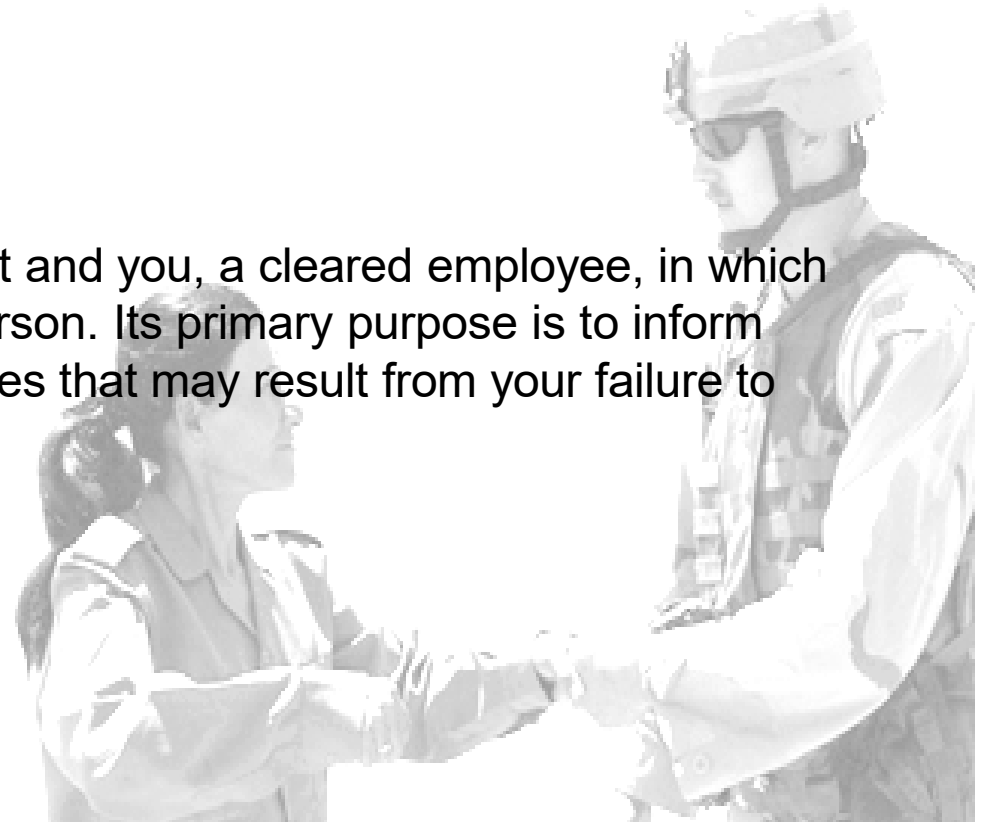# Access to Classified Information

Requirements for Access to Classified Information:

1. **Possess a valid Security Clearance**

2. **Have an official "Need-to-Know"**

3. Signed SF 312 Nondisclosure Agreement
The SF 312 is a contractual agreement between the U.S. Government and you, a cleared employee, in which you agree not to disclose classified information to an unauthorized person. Its primary purpose is to inform you of your responsibilities to protect information and the consequences that may result from your failure to meet those responsibilities.

SF 312 Overview

- I accept the obligation contained with the agreement.
- I have received a security indoctrination and a I understand my responsibility to protect classified information.
- I have been advised that unauthorized disclosure of classified information could result in damage to national security.
- I understand that I must comply with the laws protecting classified information
- I understand that a breach of the agreement could result in:
  - Termination of my clearance
  - Transfer from my position
  - Termination of my employment
  - Criminal Prosecution
- Any benefits, financial or otherwise, that I receive from the unauthorized disclosure of classified information will be given to the U.S. government.
- I understand classified information belongs to the U.S. government and not to me.
- I will return all classified materials to the U.S. government whenever I no longer need them.
- All my questions have been answered and I have been offered access to the
  Executive Order 13526 and statutes referenced in this agreement.

Contractors/Non-staff: you signed the SF 312 with your owning organization/company.

Military and Civilian Staff Member employees will sign the SF 312 prior to their first day.

Initial Security and Counterintelligence Briefing Certificate

BE SECURITY CONSCIOUS

A successful security program begins with each individual. Security needs your assistance daily to ensure that both classified and sensitive unclassified material is protected. Working together, we can make a difference.

SIGN AND DATE THE INITIAL SECURITY AND COUNTERINTELLIGENCE BRIEFING CERTIFICATE (DTRA FORM 120).

Do you hereby accept the obligations as described above and as contained in the Initial Security and Counterintelligence Briefing? If yes, please do the following:

Step 1. Sign and Date the DTRA Form 120 Initial Security and Counterintelligence Briefing Certificate.

Step 2. Email to (HQ) dtra.belvoir.oi.list.oi-mscsp-personnel-security-hqc@mail.mil
(Reston) dtra.belvoir.oi.list.oi-mscr-personnel-security@mail.mil
(ABQ) dtra.kirtland.oi.list.oi-msca-personnel-security-abq@mail.mil
(Travis) dtra.travis.oi.list.oi-msct-security@mail.mil

If you have a CAC, you may digitally sign the DTRA Forms 120 and 205. You may only exercise this option if you have a CAC. All others must sign the documents by hand.

LAN Access User Agreement

- Read pages 1-5 of the DTRA Form 205 LAN Access UserAgreement

- Sign the agreement on page 1.

Step 1. Sign and Date the DTRA Form 120 Initial Security and Counterintelligence Briefing Certificate.

Step 2. Email to (HQ) dtra.belvoir.oi.list.oi-mscsp-personnel-security-hqc@mail.mil
(Reston) dtra.belvoir.oi.list.oi-mscr-personnel-security@mail.mil
(ABQ) dtra.kirtland.oi.list.oi-msca-personnel-security-abq@mail.mil
(Travis) dtra.travis.oi.list.oi-msct-security@mail.mil

If you have a CAC, you may digitally sign the DTRA Forms 120 and 205. You may only exercise this option if you have a CAC. All others must sign the documents by hand.

UNCLASSIFIED

DTRA Information Systems Access Agreement

DTRA leadership takes security seriously and understands that poor Information System (IS) Security practices have the potential to compromise the overall mission. It is imperative that users abide by a set of standards and practices when supporting operations. This Information Systems Access Agreement coupled with acknowledgement of its underlying regulations is a foundation of the DTRA Information System Security program and is mandatory for all DTRA IS users.

Please read this document thoroughly before signing. By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) Information Systems:

You are accessing a U.S. Government information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

The information below may be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting a violation of the law. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to DTRA systems.

I attest that I have read and will abide with all criteria as stated below and I accept that failure to comply with these guidelines may subject me to disciplinary actions including loss of employment, loss of security clearances, criminal prosecution, fines, incarceration and/or UCMJ action. I have been afforded the opportunity to discuss any questions with the Information System Security Manager (ISSM) of the system(s) I am accessing.

User Name (Last, First)	Signature	Date

System User Description
A DTRA system user is defined as anyone who has access to DTRA-owned IT resources, i.e., E-Mail to include Outlook Web Access (OWA), Virtual Desktop (VDI), network shares, laptops, workstations, Smart Phones, Personal Data Assistants (PDA), software, etc. The access to these resources may be via a Virtual Private Network (VPN) type connection from external locations using DTRA supplied software and/or hardware, physical access within DTRA owned spaces, or DTRA authorized government-owned/ operated/ approved telework centers.

DTRA users play a key role in the protection of information processed by or stored on the DTRA networks. Each user is responsible for observing rules and regulations governing the secure operation and authorized use of the NIPRNET, SIPRNET, JWICS and other DTRA-owned systems and networks, as prescribed in this agreement and in DoD and National Security Directives.

You consent to the following conditions:

- The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the U.S. Government may inspect and seize data stored on this information system.
- Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
- Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by aorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense,

DTRA Form 205   MARCH 2018   (Adobe LiveCycle ES)   Page 1 of 5

Cyber and PII Training

- All new civilian employees, service members, and contractor/non-staff personnel must complete the below mandatory training requirements prior to arrival at DTRA. You may complete all training online using your personal computer.

- New Cyber Awareness Challenge (Department of Defense Version)
- Personally Identifiable Information (PII)

Step 1. Print a copy of the completion certificates
Step 2. Email to (HQ) dtra.belvoir.oi.list.oi-mscsp-personnel-security-hqc@mail.mil
             (Reston) dtra.belvoir.oi.list.oi-mscr-personnel-security@mail.mil
             (ABQ) dtra.kirtland.oi.list.oi-msca-personnel-security-abq@mail.mil
             (Travis) dtra.travis.oi.list.oi-msct-security@mail.mil

- If you experience a challenge printing the certificates, you may capture a screen shot of the completion certificate and print the screen shot.

- Note: You are not required to re-take the training if you have training certificates dated within the last calendar year

Passing Your Clearance

When you are attending a meeting/conference and need to pass your security clearance to another organization:

CIVILIAN AND MILITARY ONLY (Company Facility Security Officer (FSO) must pass contractor clearances): Submit

an outgoing visit notification to Visitor Services via the CRC https://crcportal.unet.dtra.mil/SitePages/Home.aspx

Visitors to DTRA

When you are sponsoring outside visitors to DTRA:

Whether you are hosting one, two, or 50 visitors, you should use the Visitor Notification System to let Visitor Services and Access Control know you are expecting people from outside DTRA.

Submit notification via the DTRA1, in the Customer Response Center (CRC), under Security.

Visitor Services will notify you if further information is required and will send you a confirmation when all necessary actions are completed.

Remember all Foreign visits MUST be coordinated with the Foreign Disclosure Office

Remember: IT'S POLICY!

All personnel in the below two categories must out process through Security:

1. Terminating employment, retirement, reassignment to another government agency
2. Any absence from duty or employment that exceeds 60 days. (DTRA badge and LAN will be disabled at 30 and 90 days respectively; plan in advance with Security if you know you'll be out of pocket for that period of time)

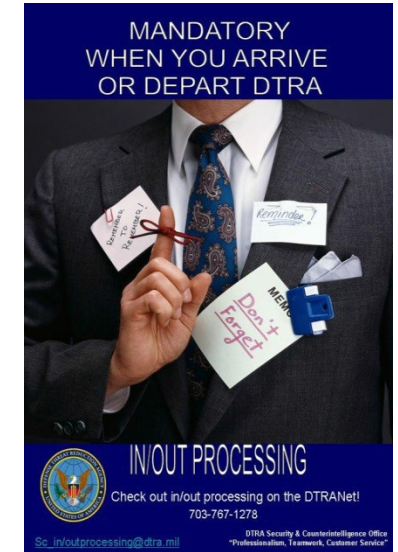**Individual Responsibility:**
If you will be leaving DTRA, notify Personnel Security by completing the Out Processing Notification located on the DTRA1 in the Customer Response Center (CRC).

Please get started a few days before you plan to leave so that all government/DTRA property is returned and accounts settled before your departure date. You must complete the majority of your out-processing prior to your actual day of departure.

YOUR LAST ACTION WILL BE SECURITY IN/OUT-PROCESSING. You must turn in all DTRA issued badges, Token, IDs, etc. DO NOT turn in your DTRA-issued badge or CAC at your company or leave them with anyone; they are the property of DTRA Security and MUST be returned to DTRA Security at the time you out process.

Any exceptions to the above process must be pre-coordinated with Security In/Out Processing by Supervisor/COTR or Security Manager.

Failure to out process may adversely affect your security clearance with another location or position.

MANDATORY WHEN YOU ARRIVE OR DEPART DTRA

IN/OUT PROCESSING
Check out in/out processing on the DTRANet!
703-767-1278
Sc_in/outprocessing@dtra.mil

DTRA Security & Counterintelligence Office
"Professionalism, Teamwork, Customer Service"

Your First Day

Ensure your government sponsor has requested an in-processing date/time for you with Personnel Security (Mil and Contractor/Non-Staff Personnel):
https://crcportal.unet.dtra.mil/SitePages/Home.aspx

*Military personnel must check in with Military HR prior to in-processing with Personnel Security

Ensure you have emailed the below documents in advance:
1. Cyber Security Awareness Training Certificate (dated within the last calendar year)
2. Personally Identifiable Information Training Certificate (dated within the last calendar year)
3. Signed DTRA Form 120
4. Signed DTRA Form 205

Security
- In-Processing w/Security
- Out-Processing w/Security
- Incoming Visit Notification
- Outgoing Visit Notification
- SIPRNET (SNET) Account Request
- JWICS Account Request
- Submit a Self-Report or Report
- Other Security Services

Questions?

Email any questions you may have to: dtra.belvoir.oi.list.oi-mscsp-personnel-security-hqc@mail.mil

WELCOME TO DTRA!