DTRA INITIAL SECURITY AND COUNTERINTELLIGENCE (CI) BRIEFING CERTIFICATE

Your assignment to, or employment by, the Defense Threat Reduction Agency (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 all applicable policies. Failure to comply with the below will be considered a failure to follow security procedures, and is reportable to the DoD CAF. Your responsibilities include the following:

DTRA BADGE. All personnel who enter a DTRA facility are required to wear a DTRA badge face-forward, above the waist, and on their outermost garment at all times within or between buildings. Remove your badge when not inside a DTRA facility or enclosed/fenced-in area, and never use it as a form of identification outside of DTRA. 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. 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. Immediately report lost or stolen badges in writing to the Security Office. Return DTRA badges to the Security Office upon completion or termination of duty.

SAFEGUARD CLASSIFIED INFORMATION. Access to classified information requires an appropriate security clearance and need-to-know. No one has a right to access classified information solely by virtue of rank or position. The final responsibility for determining whether an individual requires access to classified information, and is properly cleared, rests with the person who has possession, knowledge, or control of the information. Use appropriate cover sheets, and properly destroy classified material when no longer required. Never discuss classified material with unauthorized persons or in unauthorized spaces. Remind recipients of the classification of the information you are about to discuss. Pre-coordinate the arrival of uncleared personnel with the Security Office, and announce their presence before entering office spaces where classified information is potentially being discussed or reviewed.

THE NATO PROGRAM. All personnel requiring access to the DTRA SNET or NATO information must receive a formal NATO briefing. All NATO material will be stored separately from U.S. classified material. NATO transactions for Secret and above will be processed through the NATO registry (no exceptions).

REPORTING REQUIREMENTS. https://dtra1/j0xs/PS/Reporting/default.aspx. Reporting requirements are part of the continuous evaluation process. Your clearance eligibility includes an explicit responsibility to recognize and report behaviors, incidents, or events that could impact your (or another's) eligibility for access to classified information; failure to properly report any possible security concerns could jeopardize your security clearance and continued access. Exercise vigilance, caution, and discretion in your personal conduct to avoid placing yourself in compromising situations. Notify your cognizant Security Office or HQs Personnel Security in writing if any of the following occur:

- **Foreign travel:** Report Official and Unofficial Foreign Travel by submitting the DTRA FM 195 as soon as you are aware of the upcoming travel. Schedule a CI Foreign Travel Briefing (via email) with the Briefing/Debriefing Center no more than 30 days prior to travel. 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 contacts: Submit the DTRA FM 196. Report contacts with a known or suspected foreign intelligence entity, as well as continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact; this includes roommates, any 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 threat briefing with CI 30 days prior to expected official contact with foreign nationals within the U.S., including meetings, conferences, or symposia.
- **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
- **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.
- **Criminal conduct:** Charges, arrest (regardless of financial disposition), and traffic fines exceeding $350
- **Financial anomalies**: Report any bankruptcy, garnishment, repossessions, or attempt to collect a debt over 120 days. Any unusual infusion of assets of $10,000 or greater, such as an inheritance, winnings, or similar financial gain must also be reported. consistent with the interests of national security.
- **Alcohol and drug-related treatment.**
- **Mental Health:** Apparent or suspected mental health issues where there is a reason to believe it may impact the ability to protect classified or specifically prohibited by law from disclosure information.
- **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.

DTRA INITIAL SECURITY AND COUNTERINTELLIGENCE (CI) BRIEFING CERTIFICATE

PROHIBITED ITEMS. Cameras, weapons, wireless devices, 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.

COMMUNICATION SECURITY (COMSEC). Use of government communication systems constitutes your consent to COMSEC monitoring. Never discuss classified information or attempt to talk around it over unsecured phones or systems. Use your hold button when you are calling someone else to the phone, or when assisting a customer.

OPERATION SECURITY (OPSEC). While the need and methods to protect classified national security information are well-established, you must also be cognizant of protecting controlled (or sensitive) unclassified information. DTRA has a strict “no paper” policy: never throw any paper, regardless of classification/sensitivity, in the trash, garbage, dumpster, or recycle bin. This includes, but is not limited to, paper, notebook paper, post-its, scratch pads, calendar sheets, etc.

This form covers your basic DTRA security-related requirements and obligations: DTRA Badge, Safeguarding Classified Information, Prohibited Items, NATO Program, Reporting Requirements, COMSEC, and OPSEC. Contact your cognizant Security Office to view and applicable references or policy documents.

Your signature below indicates you have read, understand, agree to the terms, and accept the obligations outlined herein (DTRA Form 120, pages one and two)

PRINT NAME	SIGNATURE	DATE
		4/23/24