DSCA INITIAL SECURITY BRIEFING CERTIFICATE

Your assignment to, or employment by, the Defense Security Cooperation Agency (DSCA) carries responsibilities for safeguarding all classified and sensitive unclassified information you may come in contact with. You are responsible for helping maintain DSCA'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:

COMMON ACCESS CARD (CAC) & DSCA BADGE. All personnel who enter a DSCA facility are required to wear a DSCA badge face-forward, above the waist, and on their outermost garment at all times. Remove your badges when not inside a DSCA facility, and never use it as a form of identification outside of DSCA. Escort any individual within a DSCA facility who is not wearing a DSCA badge, or unescorted individuals wearing a red ESCORT REQUIRED badge to Access Control. Never allow other personnel to use your CAC or DSCA 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 CAC and DSCA badge 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.

REPORTING REQUIREMENTS. 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 to classified information. 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 OCONUS DSCA Travel Notification Form no later than 10 working 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:** 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 to the DSCA Personnel Security Specialist.
- **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 authorized 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.
- **Media contacts:** Any release of DSCA information, to the media or otherwise, must be approved through the DSCA 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 disdosure. If any member of the media contacts you for information, refer them to Public Affairs; never comment on news releases pertaining to DSCA 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.

DSCA INITIAL SECURITY BRIEFING CERTIFICATE

PROHIBITED ITEMS. Cameras, weapons, wireless devices, and other portable electronic devices are not permitted within DSCA 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. DSCA NIPR 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, please contact DSCA Cyber Security for approved list. Connecting to DSCA systems or networks is prohibited. DSCA 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.

This form covers your basic DSCA security-related requirements and obligations: DSCA Badge, Common Access Card, Safeguarding Classified Information, Prohibited Items, 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 (DSCA Form 120, pages one and two).

_____	_____	_____
PRINT NAME	SIGNATURE	DATE

SECURITY AND FACILITIES DIRECTORATE ONLY: ACCEPTANCE

_____	_____	_____
PRINT NAME	SIGNATURE	DATE