NATIONAL ACADEMIES *Sciences Engineering Medicine*

OFFICE OF PROGRAM SECURITY

OSEC Frequently Asked Questions

1. Q: Why must I complete the Annual Security Refresher Briefing security training every year?

   A: Security training is an **annual requirement** per 32 C.F.R. 117.12(k). This training must include key security concepts & responsibilities such as: handling classified information, reporting requirements, insider threat, derivative classification, legal consequences for misconduct, etc. Security offices must maintain a record of training completion for each cleared individual. *If you have already **completed** an ASRB training **this calendar** year with your home organization, we will accept a **qualifying** training. This training must be completed before the OSEC training deadline assigned and must cover all required material.

2. Q: What is "Formstack" and why am I directed to this site for certain document transmission?

   A: Formstack is the designated platform for secure collection of personally identifiable information (PII) necessary for OSEC reporting and compliance actions. Formstack meets the compliance standard for protection of PII including but not limited data encryption and access controls. (For questions about the system, please contact OSEC_IT@nas.edu).

3. Q: Do I really have to report **all** my foreign travel?

   A: Yes, per 32 C.F.R § 117.8, all cleared personnel must submit foreign travel reports and receive any pre-travel briefings and post travel briefings from their security office. (If you already report foreign travel with your home organization, we will accept those reporting forms in place of our OSEC forms so long as the forms capture the required reporting information.)

4. Q: What can't I download CUI?

   A: The NAS CUI Enclave (Microsoft GCCH) system is the designated platform for CUI access under our contract activities. Your personal and/or work devices are not within our control boundary. We are not able to see or access these devices to ensure CUI program compliance. Keeping the CUI within our accredited system, meets our CUI requirements, protects NAS, and ensures your personal/work devices are not subject to audit.

5. Q: When does my clearance 'expire'?

   A: Short answer, 1.) when the contract activity concludes, 2.) the individual is no longer performing on the project, or 3.) the clearance is revoked or suspended by the sponsor agency. Per 32 C.F.R § 117.10 clearance is only in place so long as there is active U.S. government contract in place requiring classified access.

6.a. Q: What is Continuous Vetting and why have I been asked to complete another SF-86?

   A: Continuous Vetting (CV) is a process that involves regularly reviewing a cleared individual's background to ensure they continue to meet security clearance requirements and should continue to hold positions of trust. Enrollment in the program requires an individual to update their SF-86 Questionnaire for National Security Positions every 5 years.

6.b. Q: How does the Continuous Vetting (CV) process work?

   A: Automated record checks pull data from criminal, terrorism, and financial databases, as well as public records, at any time during an individual's period of eligibility. When the sponsor agency receives an alert, it assesses whether the alert is **valid** and **requires further investigation**. The sponsor agency then makes a clearance determination. CV helps the sponsor agency mitigate personnel security situations before they become larger problems, either by working with the cleared individual to mitigate potential issues, or in some cases suspending or revoking clearances.

7. Q: I have been invited to a classified meeting at another facility and need OSEC to verify I have a clearance, why do I need a to complete a "Visit Authorization Requestion (VAR) Form"?

A: Each time you enter a cleared facility, your current clearance eligibility must be verified with a visit authorization letter (VAL) from one facility to another. A VAR form is required on our end to ensure the classified visit is approved by your project RSO, related to your contract activity, and has the required information for submission. ***SCI level visits also requires USG sponsor approval*.**

8. Q: Why can't I take my unclassified notes with me at the end of a classified meeting?

   A: As a default, NAS does not permit unclassified notetaking during classified sessions. This approach protects our volunteers and staff from risks of mismarking/mishandling information which can result in serious security violations and loss of clearance. Authorization to take unclassified notes during a classified session has been granted in limited cases where the sponsor agency has explicitly authorized it and other required conditions were met.

9. Q: This information is available all over the internet, why can't I reference it in my work?

   A: From Wikileaks, to Manning, from Snowden to Teixeira – classified information can sometimes enter the public domain. Cleared individual have a responsibility not to cite, quote, or reference classified information in the public discourse. The only appropriate response if confronted with information you know to be classified in the public – "No comment." Then immediately report it to your security office.

10. Q: I am scholar, not an intelligence or military professional, I can't seriously be a target for foreign adversaries, can I?

    A: As an academic, you are most likely to be approached via **Academic Solicitation**. This technique is one of the fastest growing methods of operation reported by cleared contractors. Academic Solicitation is "the use of students, professors, scientists, or researchers as collectors improperly attempting to obtain sensitive or classified information."

11. Q: I am former military or intelligence professional, I know all of this information. Why does this information matter to me?

    A: As a former military or intelligence professional, you are most likely to be approached via **job solicitation** or **professional social media site** (e.g. LinkedIn). Be cautious about sharing details of your past government work. Best practice is to contact your previous government employer to 1.) have your resume submitted for security review, and 2.) request a security briefing through your prior agency's security office.

12. Q: My assistant reached out for my login information for CUI access and was denied. This individual is authorized to access this type of information with our home organization, what is the problem?

    A: The NAS CUI Enclave (Microsoft GCCH) system is the designated platform for CUI access under our contract activities. This access is specific to committee and staff member performing under the contract activity. Assistants, co-workers, student, etc. are not permitted to receive or use an unauthorized user's login credentials.

13. Q: I'm ready to log-in on the classified IT system and I am handed a packet of training I believe I have already completed. Why am I being asked to complete additional forms?

    A. Before accessing any classified IT system, you must complete an 1.) information system user agreement acknowledging the rules for accessing that particular system, 2.) a derivative classifier training on marking classified information, and 3.) an insider threat refresher. **All training and agreements must renewed every 12 months**.

14. Q: Insider Threat reporting sounds like "big brother" to me. Why would I want "snitch" on a fellow committee member or staff member? Tattling is not my job.

    A. Insider threat reporting is vital part of a **healthy**: security program, corporate culture, risk management effort, and even employee wellness program. Oftentimes insider threat behavior is either a consequence of lack of awareness of organizational rules or symptomatic of stressors which would benefit human resources support. **If you see something, say something**…before a colleague's "misstep" becomes something more serious.