**OPSEC DEFINITION****:** OPSEC is a systematic way of identifying and mitigating risk to (insert organization) operations by assessing how we as an organization may inadvertently disclose sensitive or **critical information** that is desirable to adversaries and competitors.

**CRITICAL INFORMATION:** Critical information consists of specific facts about (insert organization) capabilities and developments that are vitally needed by adversaries or competitors to ensure our mission failure or compromise. To prevent compromise, (insert organization) as an organization must first determine what is critical or sensitive within our work that requires safeguarding.

**(5) STEPS FOR IDENTIFICATION AND PROTECTION OF CRITICAL INFORMATION:**

1. **Set the Organizational Boundaries**. Determine which organization, partners, or sub-organizations uses or accesses the information whose sensitivity is in question.

2. **Determine Critical Information Components**. Assess which – or all -- of the (insert organization) operations, projects, programs, and partners, include sensitive or critical information. Consider personnel, facilities, infrastructure, Research, Development, Testing, Evaluation, and Production (RDTE&P) of Sensitive Technology (or Commodities), and conduct of sensitive negotiations.

3. **Understand the Threat.** (insert organization) may have several competitors, both foreign and domestic. Who are (insert organization) adversaries and how are they capable of impacting (insert organization) operations?

4. **Consider the Sources.** Make a list of the internal and external sources involved in (insert organization) operations that might include Critical Information and potential opportunities for disclosure. Examples of Sources include telecommunications, virtual engagements, paper documents, press releases, visitors, stored data, social media accounts, etc.

5. **Assess Vulnerabilities.** Review (insert organization) Physical, Personnel, and Communications Security policies to identify gaps in capabilities and potential opportunities for compromise. Consider access-control, personnel, and communications vulnerabilities. What additional security measures are required to safeguard critical information and its’ sources?

**OPSEC RESPONSIBILITIES:** Every (insert organization) member is responsible for the security of the information. Disclosure of (insert organization) critical information may directly impact organizational goals. Leaders at all levels are integral in enforcing OPSEC by ensuring:

1. Avoid openly posting or discussing schedules that may reveal critical information.
2. Ensure members review (insert organization) Critical Information as part of security training.
3. Coordinate threat briefs for all new and existing members to include how to identify and report any attempts by unauthorized personnel to solicit sensitive or critical information.
4. Ensure official information intended for the public receives a security review prior to release.
5. Protect from disclosure any critical information and sensitive information to which they have personal access, including a) Maintain need-to-know, document classification markings, and Limit distribution procedures; b) Refrain from talking about operations in public locations; c) Safeguard transmission of physical and digital critical information, including storage, transmission, and disposal met

**COMMUNICATIONS SECURITY RECOMMENDATIONS FOR THE WORKPLACE:** Organizational Critical Information should not be discussed over an unsecured telephone. If it is necessary to discuss classified or critical information, ensure employees use secure communications as the only authorized means for discussion.

1. Make maximum use of secure communications, telephone, fax, email and text messages. **Use encryption devices whenever possible, particularly when transmitting critical information.**

2. Limit release of critical information until latest possible date or until activities are completed and only by authorized personnel.

3. Control distribution of non-classified, sensitive information in accordance with distribution markings for technical and operational information.

|  |  |
| --- | --- |
| **VTC/Telecon** | **Email / Encryption Instructions** |
| -Use tools with end-to-end encryption​  -Ensure host has visibility and control over all participants​  -Use phone as a last resort only  **Microsoft Teams**​ (USG Internal)  **Cisco Webex** (for phone options and/or external participants)  -Identify each unidentified phone caller before starting the meeting​  -Remove anyone from meetings who can't be identified​ | Digitally sign & encrypt email as default​:  -Select **File** > **Options** > **Trust Center** > **Trust Center Settings**. ​  -In the left pane, select **Email Security**.​  -Under **Encrypted email**, ensure the first two boxes are checked, then click **Publish to GAL…** and follow prompts.​  ​***If you get a warning that you cannot encrypt to a given recipient, ask user to send a digitally signed email and then add user to address book*** |

