Purpose

This framework serves as tool to move beyond compliance and become a steadfast guardian of our Nation's security. Use it to sharpen your instincts, transform your everyday actions, and forge a stronger culture of security in the workplace.

The 5-R Security Awareness Framework

PRINCIPLE	ACTION
REVIEW 	Develop the skillset to **Review** the regulatory guidance through the lens of scanning your environment and the actions of others for harmful behaviors and indicators.
RECOGNIZE 	Hone your ability to **Recognize** a security issue and promote a security awareness culture.
REACT 	Develop the instinct to **React** and respond appropriately and decisively to everyday security challenges.
REFERENCE 	Determine how to identify and locate the regulatory guidance and other applicable security resources so you can **Reference** it when necessary.
REPORT 	Determine reporting requirements: understand your duty to **Report,** know what to report, who to report to, and when, in accordance with required procedures.

The 5-R Framework Security Awareness Framework in Practice

Scenario Background: David is a DOW civilian project lead responsible for a new command and control software suite. Alex is another DOW civilian employee recently assigned to David's team. Alex is known for being sharp and technically skilled but has a reputation for cutting corners.

1. Review

The scenario begins with David leaving his mandatory annual security briefing. The core message is fresh in his mind: "Review the regulatory guidance through the lens of scanning your work environment and the actions of others for harmful behaviors and indicators."
On his way back to his desk, he passes a common area and sees Alex talking animatedly on his personal cell phone. David overhears Alex mentioning specific server codenames and a known bug in their project's code.

- David's Thought Process (Review): *The Operations Security (OPSEC) briefing just covered this. We are not supposed to discuss Controlled Unclassified Information (CUI) in non-secure areas or on personal devices. Those server names aren't classified, but they are designated as CUI - OPSEC and are on the organization's Critical Information List (CIL). Alex is creating an intel-gathering opportunity for anyone who can overhear.*

David is actively reviewing the environment and Alex's actions against the security guidance he just received.

2. Recognize

A few hours later, David sees Alex at his workstation, holding a small, personal USB drive. "I have a bunch of useful scripts on this drive from my last project," Alex tells him. "It'll be faster than pulling them from the shared drive."

- David's Thought Process (Recognize): *Okay, that's the second time. First, the unsecured phone call, and now prohibited removable media. This isn't just a one-off mistake; this is a pattern. Alex is prioritizing convenience over fundamental security policies.*
  I recognize this as a significant security issue and a threat to the security culture of our team.

David's focus shifts from observing a single mistake to recognizing a dangerous pattern of behavior.

3. React

That same afternoon, David is leaving the secure workspace and badges out. Alex, walking behind him without his badge, calls out, "Hey man, hold the door for me!"

- David's Action (React): David lets the heavy door close firmly behind him, ensuring it locks. He gives Alex a neutral look and says, "Sorry, you know the rule. Everyone has to badge out individually."

His instinct is to react decisively to protect the integrity of the secure area. He doesn't lecture, but he also doesn't comply. He denies the immediate request, preventing the security breach, and decides his next step must be more formal.

4. Reference

Back at his desk, David knows he needs to report this pattern. Before he does, he wants to ensure his report is precise and fact-based.

- David's Action (Reference): He opens his workstation and navigates to the Washington Services Headquarters website, where he can access the most recent DOW regulatory guidance on CUI, access controls, and removable media. There is no way to memorize all the regulations, but David knows how to locate and identify the regulations to validate his concerns.
    1. DOD Instruction 5200.48, “Controlled Unclassified Information, to confirm the procedures for protecting CUI in accordance with DOW regulatory guidance.
    2. DOD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)" which contains specific regulatory guidance on removable media and USB ports.
    3. DOD Manual 5200.01, Volume 3, "DOD Information Security Program: Protection of Classified Information.”

He knows where to go to locate and reference the official guidance, allowing him to ground his concerns in accordance with specific policy, not just opinion.

5. Report

With his facts straight and the relevant policies referenced, David knows he has a duty to report.

- David's Action (Report): He contacts his direct supervisor and his activity’s security manager. He provides a concise, factual report:

- What: He details the three incidents: the discussion of CUI on a personal phone, the attempted use of removeable media, and the attempt to bypass access controls or piggyback.
- Who: He identifies Alex as the individual involved.
- When: He provides the dates and approximate times of each incident.

He understands his duty to report the security incidents promptly and to the correct authorities.

The Payoff

David's implementation of the 5-R Security Awareness Framework reinforces the importance of becoming a vigilant security proponent. He went beyond the baseline and honed his instincts to help forge a stronger culture of security in the workplace.