Cybersecurity Working Group

Council of the Inspectors General on Integrity and Efficiency
Executive Newsletter October 2022

IN THE NEWS

If the U.S. Loses the War for Cyber Talent, It Loses the Cyberwar

The global cost of cyberattacks is expected to reach $10.5 trillion by 2025. And over 620 million ransomware attacks were recorded in 2021 alone. The cybersecurity industry has responded to this threat by unleashing a wave of innovation, and we saw $29.5 billion in venture capital funding pour into cybersecurity. There are over 714,000 unfilled cybersecurity positions in the U.S. Without appropriately trained personnel, organizations cannot properly implement and manage the many cybersecurity tools coming to market.

White House Targets 3 Critical Infrastructure Sectors for New Cyber Regulations

White House Deputy National Security Adviser Anne Neuberger said Thursday that communications, water, and healthcare are the next critical infrastructure sectors the Biden administration plans to work with to increase their baseline cybersecurity. The effort, which will be carried out by various federal agencies, is the latest step by the administration to seal gaps in the security of critical infrastructure against hackers.

CYBER-JARGON

- Penetration Testing (pen tests)- is a method of checking for security weaknesses in software and systems by simulating real-world cyber-attacks. Pen tests find gaps in protection that can arise when unique combinations of applications, systems, and security defenses work together in live environments.

- Red/Blue/Purple team engagements–These are structured attack and defend scenarios where a red team made up of penetration testers targets a defensive blue team's assets. Red team engagements stress test threat detection and response aptitude of the blue teams in realistic scenarios. When these teams work more collaboratively, it is referred to as a purple team test.

TOPICS OF INTEREST

8 Hallmarks of a Proactive Security Strategy

CISOs have long been tasked with building response and recovery capabilities, the objective being to have teams that can react to a security incident as quickly as possible and can restore business functions with as little damage as possible. However, a proactive strategy can do much more to ensure organizational resiliency than focusing solely on rapid response once an attack or breach has been detected.

RECENT OIG WORK (OVERSIGHT.GOV)

U.S. Citizenship and Immigration Services (USCIS) Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information (opens a PDF)

The Department of Homeland Security conducted this audit to determine the extent to which USCIS applies IT access controls to restrict unnecessary access to systems and information.

IMPORTANT DATES

Binding Operational Directive (BOD) 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks

By April 3, 2023, agencies must:

- ✓ Perform automated asset discovery every seven days.
- ✓ Initiate vulnerability scans across all discovered assets every 14 days.
- ✓ Display vulnerability results in the Continuous Diagnostics and Mitigation (CDM) dashboards within 72 hours of automated discovery.
- ✓ Develop and maintain the capability of on-demand asset discovery and vulnerability scans within 72 hours of CISA requests and provide CISA the results within seven days.
- ✓ Deploy an updated CDM Dashboard configuration that shows vulnerabilities at the object level for CISA analysts.

There is a more detailed biweekly version of this newsletter available. Sign-up by emailing: <cmitchell@oig.doc.gov>