IDS WG Meeting Minutes
January 12, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on January 12, 2023.

Attendees

Gerardo Colunga	HP
Alan Sukert	
Mike Trent	Xerox
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Special topic on the Cybersecurity Incident and Vulnerability Playbooks developed by CISA (Cybersecurity & Infrastructure Security Agency) as part of the response to the 2021 Executive Order of Cybersecurity
   - Open Discussion on what IDS should focus on in 2023
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust-policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al presented this week's special topics on the Cybersecurity Incident & Vulnerability Response Playbooks - Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems. The slides Al used can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/Incident and Vulnerability Response Playbooks.pdf and the text of the Cybersecurity Incident & Vulnerability Response Playbooks can be found at https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

   The main items covered in the presentation were:
   - As indicated above, the Cybersecurity Incident & Vulnerability Response Playbooks were issued in February 2021 by CISA in response to the 2021 Executive Order on Cybersecurity, The scope of these playbooks is:
     - Provide Federal Civilian Executive Branch (FCEB) agencies with a standard set of procedures to identify, coordinate, remediate, recover, and track successful mitigations from incidents and vulnerabilities affecting FCEB systems, data, and networks.

     This means that the playbooks apply to the entire Executive Branch of the US Government. Incidents covered by the playbooks can be initiated from both inside and external to each applicable FCEB.

     Al noted that the Incident Response Playbook only apply to incidents that involve confirmed malicious cyber activity and for which a major incident has been declared or not yet been reasonably ruled out – this means that only major incidents that either have actually occurred or analysis has not totally confirmed that it has occurred (but the possible occurrence has not been ruled out). That somewhat limits the scope of the Playbooks use, but not as much as one might think.

     The Vulnerability Response Playbook only applies to vulnerabilities being actively exploited.
   - A few important terms to understand what is in the two playbooks are:
     - **FCEB Agencies**: Federal Civilian Executive Branch Agencies (FCEB Agencies) include all agencies except for the Department of Defense and agencies in the Intelligence Community

  - **Incident**: An occurrence that— (A)actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B)constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies
  - **Major Incident**: Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. .Agencies should determine the level of impact of the incident by using the existing incident management process established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide, **or** A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people
  - **Vulnerability**: The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control

  The definition of ‘Major Incident” is significant in that it encompasses not just incidents that can impact national security, but incidents that can impact health and safety, privacy and the economy. That means the scope of the Incident Response Playbook is much broader than it would appear to be initially.

- The Incident Response Playbook is intended to “a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2, Computer Incident Handling Guide” and to describe process FCEB agencies should follow for confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.

  Slide 7 gives a pictorial view of the Incident Response Process described in the Incident Response Playbook. The process has 6 phases:

  - Preparation
  - Detection & Analysis
  - Containment
  - Eradication & Recovery
  - Post-Incident Activity
  - Coordination

  It is interesting, given that the contents of the Incident Response Playbook are based on NIST SP 800-61R2, that the incident response process covered in NIST SP 800-61R2 has 4 phases:

  - Preparation
  - Detection & Analysis
  - Containment Eradication & Recovery
  - Post-Incident Activity

  In NIST SP 800-61 Coordination is not treated an Incident Response Process phase, although a whole chapter of the standard is devoted to Coordination issues.

  The discussion of each phase in the Incident Response Playbook is as follows:

  a. Preparation Phase

     The Preparation phase defines baseline systems and networks before an incident occurs to understand the basics of “normal” activity. Establishing baselines enables deviations.

     Preparation also involves activities such as:

- Having infrastructure in place to handle complex incidents, including classified and out-of-band communications,
- Developing and testing courses of action (COAs) for containment and eradication, and
- Establishing means for collecting digital forensics and other data or evidence

The key activities in the Preparation phase are:

- Develop and implement Incident Response Policies and Procedures
- Develop and maintain an accurate picture of infrastructure (systems, networks, cloud platforms, and contractor-hosted networks)
- Train personnel to respond to cybersecurity incidents
- Actively monitor cyber intelligence feeds for threat or vulnerability advisories from government, trusted partners, open sources, and commercial entities
- Establish active defense capabilities—such as the ability to redirect an adversary to a sandbox or honeynet system for additional study
- Establish local and cross-agency communication procedures and mechanisms for coordinating major incidents with CISA and other sharing partners
- Take steps to ensure that IR and defensive systems and processes will be operational during an attack
- Implement capabilities to contain, replicate, analyze, reconstitute, and document compromised hosts; implement the capability to collect digital forensics and other data
- Leverage threat intelligence to create rules and signatures to identify the activity associated with the incident and to scope its reach

The main activities of the Preparation phase involving developing and implementing the proper procedures, resources and tools in place to effectively implement the other process phases. However, maybe the most important activity in this phase revolves around establishing a baseline of the normal configuration and behavior of the system when it is in a typical operational state. Unless there is a good documentation and categorization of the “normal” state of the system when in operational mode, one will not be able to easily tell if or when the system is in an “abnormal” state.

b. Detection & Analysis Phase

The main goals of this phase are to:

- Accurately detect and assess cybersecurity incidents
- Determine whether an incident has occurred and, if so, the type, extent, and magnitude of the compromise within cloud, operational technology (OT), hybrid, host, and network systems
- Implement defined processes, appropriate technology, and sufficient baseline information to monitor, detect, and alert on anomalous and suspicious activity.
- Ensure there are procedures to deconflict potential incidents with authorized activity

This last goal is important, because there may be instances where an incident turns out to be due to some type of human or equipment error, and you want to be able to resolve the incident without causing some type of inter-department or inter-government squabble.

The main activities for the Detection & Analysis phase are:

- Declare an incident by reporting it to CISA at https://www.us-cert.cisa.gov/ and alerting agency IT leadership to the need for investigation and response
- Identify the type of access, the extent to which assets have been affected, the level of privilege attained by the adversary, and the operational or informational impact
- Collect and preserve data for incident verification, categorization, prioritization, mitigation, reporting, and attribution

- Develop a technical and contextual understanding of the incident
- Acquire, store, and analyze logs to correlate adversarial activity
- Assess and profile affected systems and networks for subtle activity that might be adversary behavior
- Identify the root cause of the incident and collect threat information that can be used in further searches and to inform subsequent response efforts
- Identify the conditions that enabled the adversary to access and operate within the environment
- Compare TTPs to adversary tactics, techniques & procedures (TTPs) documented in the MITRE ATT&CK® framework and analyze how the TTPs fit into the attack lifecycle (TTPs describe “why,” “what,” and “how.”)
- Identify any additional potentially impacted systems, devices, and associated accounts
- Obtain Third-Party support if needed
- Use its developing understanding of the adversary’s TTPs to modify tools to slow the pace of the adversarial advance and increase the likelihood of detection

These activities are what one would normally expect once an incident has been determined to have occurred – determine the nature of the incident, collect all the data possible about the incident itself, how the vulnerability(ies) or threat was exploited to cause the incident to occur and the threat actor involved, the impacts of the incident, and determine, if possible, the root cause of the incident.

c. Containment Phase

The goal of this phase is to prevent further damage and reduce the immediate impact of the incident by removing the adversary’s access

Some things that need to be considered in determining a containment strategy are:

- Any additional adverse impacts to mission operations and availability of services
- Duration of the containment process
- Resources needed, and effectiveness (e.g., full vs. partial containment; full vs. unknown level of containment)
- Any impact on the collection, preservation, securing, and documentation of evidence

The main activities of this phase are:

- Isolating impacted systems and network segments from each other and/or from non-impacted systems and networks
- Capturing forensic images to preserve evidence for legal use (if applicable) and further investigation of the incident
- Updating firewall filtering
- Blocking (and logging) of unauthorized accesses; blocking malware sources
- Closing specific ports and mail servers or other relevant servers and services.
- Changing system admin passwords, rotating private keys, and service/application account secrets where compromise is suspected and revocation of privileged access
- Directing the adversary to a sandbox (a form of containment) to monitor the actor’s activity, gather additional evidence, and identify attack vectors
- Ensure that the containment scope encompasses all related incidents and activity — especially all adversary activity

It is important that containment encompass all of these activities so that once contained you not only minimize the impact of the incident but also help minimize the possibility of the incident reoccurring.

d. Eradication & Recovery Phase

The goal of this phase is to eliminate any artifacts of the incident (e.g., remove malicious code, re-image infected systems) and mitigate the vulnerabilities or other conditions that were exploited, so that the system can return to a “normal” state. In doing this it is important that all means of persistent access into the network have been accounted for, that the adversary activity is sufficiently contained, and that all evidence has been collected.

The main activities of this phase are:

- Develop and execute the Eradication Plan so that actions to eliminate all evidence of compromise and prevent the threat actor from maintaining a presence in the environment can be taken. Note that the last part of this is critical because in many exploits the threat actor may access the system for long periods of time, so it is critical that part of eradication is ensuring that the threat actor no longer has access to the system involved.
- Ensure evidence has been preserved as necessary
- Continue with detection and analysis activities to monitor for any signs of adversary re-entry or use of new access methods
- Restore systems to normal operations and confirm that they are functioning normally
- Ensure that have enhanced vigilance and controls in place to validate that the recovery plan has been successfully executed and that no signs of adversary activity exist in the environment

Preserving evidence is very important for legal and to help facilitate the two remaining phases.

e. Post-Incident Phase

This phase involved activities associated with documenting the incident, informing agency leadership, hardening the environment to prevent similar incidents, and applying any lessons learned to improve the handling of future incidents

The main activities for this phase are:

- Add enterprise-wide detections to mitigate against adversary TTPs that were successfully executed during the incident
- Identify and address “blind spots” to ensure adequate coverage moving forward
- Closely monitor the environment for evidence of persistent adversary presence
- Provide post-incident updates as required by law and policy
- Conduct a lessons-learned analysis to review the effectiveness and efficiency of incident handling

The two key activities in Al’s view are the ones associated with (1) making sure the information obtained about the incident, its containment and its eradication are made know across the entire organization and (2) doing the lessons learned so the entire organization can learn from what went right and what didn’t for this incident.

f. Coordination Phase

The goal of this phase is to ensure that FCEB agency experiencing the incident and CISA coordinate early and often throughout the response process

The key activities for this phase are:

- Coordinate with CISA throughout the various Incident Response phases
- Perform intergovernmental coordination based on the roles and responsibilities of the Federal agencies that need to be involved.

- The goals of the Vulnerability Response Playbook are to:

- Standardize the high-level process that agencies should follow when responding to urgent and high-priority vulnerabilities,
- Ensure that agencies, including CISA, can understand the impact of these critical and dangerous vulnerabilities across the federal government,
- Ensure that effective vulnerability management practices are being followed and
- Have a process in place to understand the relevance of vulnerabilities to the environment by tracking operating systems and other applications for all systems

The third of the four goals is the one that best ties to the Executive Order on Cybersecurity, which requires as part of the requirements for protecting the software supply chain that the government develop “a vulnerability disclosure program that includes a reporting and disclosure process”.

Slide 21 pictorially shows Vulnerability Response process that is described in the Vulnerability Response Playbook. The four phases of the Vulnerability Response process are:

- Identification
- Evaluation
- Remediation
- Reporting

The discussion of each phase in the Vulnerability Response Playbook is as follows:

a. Identification Phase

The Identification Phase the main activities are to:

- Proactively identify reports of vulnerabilities that are actively exploited in the wild by monitoring threat feeds and information sources and
- Capture additional information about the vulnerability to help with the rest of the Vulnerability Response process. This can include information such as the severity of the vulnerability, susceptible software versions, and indicators of compromise (IOCs) or other investigation steps that can be used to determine if it was exploited.

The identification of vulnerability information can come from sources both within and outside of the government such as the US-CERT, CISA’s Binding Operational Directive (BOD) 22-01, Managing Unacceptable Risk of Known Vulnerabilities, National Vulnerability Databases or from the various FCEB agencies as they detect potential or actual vulnerabilities in their systems. .

b. Evaluation Phase

The Evaluation Phase, the FCEB agency determines whether the vulnerability of interest exists in the environment and how critical the underlying software or hardware is. If the vulnerability exists in the environment, the vulnerability is addressed to determine whether it has been exploited in the agency's environment.

If the vulnerability was exploited in the environment, the FECB agency should immediately begin the incident response activities as described in the Incident Response Playbook.

At the end of the Evaluation phase, the goal is to understand the status of each system in the environment as:

- **Not Affected.** The system is not vulnerable.
- **Susceptible.** The system is vulnerable, but no signs of exploitation were found, and remediation has begun
- **Compromised.** The system was vulnerable, signs of exploitation were found, and incident response and vulnerability remediation has begun

c. Remediation Phase

In the Remediation Phase the principal activity is to remediate all actively exploited vulnerabilities that exist on or within the environment in a timely manner. In most cases, remediation should consist of patching.

If patching is not possible there are other potential mitigations that may be appropriate such as:

- Limiting access
- Isolating vulnerable systems, applications, services, profiles, or other assets
- Making permanent configuration changes

In cases where patches do not exist, have not been tested, or cannot be immediately applied promptly, there are other courses of action that can be used to prevent exploitation such as:

- Disabling services
- Reconfiguring firewalls to block access
- Increasing monitoring to detect exploitation

An important activity of this phase is to keep track of their status for reporting purposes as systems are remediated. Each system should be able to be described as one of these categories:

- **Remediated.** The patch or configuration change has been applied, and the system is no longer vulnerable or
- **Mitigated.** Other compensating controls—such as detection or access restriction—are in place and the risk of the vulnerability is reduced or
- **Susceptible/Compromised.** No action has been taken, and the system is still susceptible or compromised.

d. Reporting Phase

In the Reporting Phase the main activities are to:

- Share information about how vulnerabilities are being exploited by adversaries to help defenders across the federal government understand which vulnerabilities are most critical to patch,
- Ensure CISA maintains awareness of the status of vulnerability response for actively exploited vulnerabilities and
- Report to CISA in accordance with Federal Incident Notification Guidelines, Binding Operational Directives, or as directed by CISA in an Emergency Directive

The sharing of vulnerability information is critical to ensuring the detected vulnerabilities in one FECB agency are not repeated in the other FECB agencies. Also, different agencies may have vulnerability information, that when shared, can be put together to see the “big picture” that a single agency may not be able to see.

At the end of the presentation on the two playbooks, Bill asked who will do all of these incident and vulnerability response activities. Al’s answer was that since these playbooks are strictly intended for FECB agencies, it will be up to each FECB agency to provide the resources to accomplish the incident and vulnerability response activities. That could be done by in-house manpower, but more likely it would be done by a combination of in-house and outsourced resources; however, it will still be each FECB agency’s responsibility to ensure the various activities are done for that agency.

Whether or not the various FECB agencies in the Executive Branch are actually using the two playbooks for incident and vulnerability response is another question Al i=did not know the answer to, but he suspected most are probably not following the two playbooks.

- After finishing the discussion of the Incident Response and Vulnerability Response Playbooks, Al briefly discussed NIST SP 800-61R2 which can be found at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

  Al presented a pictorial view of the Incident Response process, as defined in NIST SP 800-61R2, that shows the differences in the phases in the Incident Response process described in NIST SP 800-61R2 from the Incident Response process described in the Incident Response Playbook, as discussed above.

  Al did not go into detail of the Incident Response process phases as described in NIST SP 800-61R2 – that is a presentation possible for a future IDS WG meeting. Instead, Al presented two recommendation slides.

  The first slide had the NIST general incident handling recommendations:

  - Acquire tools and resources that may be of value during incident handling
  - Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure
  - Identify precursors and indicators through alerts generated by several types of security software
  - Establish mechanisms for outside parties to report incidents
  - Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems
  - Profile networks and systems
  - Understand the normal behaviors of networks, systems, and applications
  - Create a log retention policy
  - Perform event correlation
  - Keep all host clocks synchronized

  Precursors are signs that an incident may occur in the future; Indicators are signs that an incident may have occurred or may be occurring now. Also, synchronization is important so that any timelines can be properly constructed for an incident. These recommendations also enforce a key point in the Incident Response Playbook for the Preparation Phase of the importance to establish a baseline of system configuration and behavior in normal operating mode.

  The second slide had the following NIST recommendations for coordination and information sharing (keep in mind in NIST SP 800-61R2 'Coordination' is not considered a phase of the Incident Response process):

  - Plan incident coordination with external parties before incidents occur
  - Consult with the legal department before initiating any coordination efforts
  - Perform incident information sharing throughout the incident response life cycle
  - Attempt to automate as much of the information sharing process as possible
  - Balance the benefits of information sharing with the drawbacks of sharing sensitive information
  - Share as much of the appropriate incident information as possible with other organizations

  Consulting with Legal is important to make sure coordination follows any applicable laws and regulations. The other key recommendation is to make sure coordination happens throughout the Incident Response process.

4. The last item on the agenda was an open discussion on what the IDS WG should pursue in 2023. The members present indicated that the important items IDS should pursue in 2023 are:
   - Continue following the work of the HCD iTC, although now that HCD cPP v1.0 and HCD SD v1.0 have been published the nature of what the HCD iTC will be doing will be changing in 2023.

     There will be two major activities the HCD iTC will be focusing on in 2023:
     - Determining the content of the next versions (probably v1.1) of the HCD cPP and HCD SD. No release plan has yet been agreed upon by the HCD iTC, although it was agreed that there will be major and minor releases and the next releases of the cPP and SD will be a minor release. A couple of areas that will likely cause new or revised content in the cPP and SD are the changes made in CC2022 Part 2 and the new/modified content in NDcPP v3.0; Al has been looking at both of these and will share his findings at a future IDS WG meeting.
     - Setting up and implementing the HCD Interpretation Team (HIT) to address questions, comments and issues found in the published version (v1.0) of the HCD cPP and HCD SD.
   - Follow the work being done by the PWG and by industry regarding the security of 3D printing. 3D printing is becoming main stream now, as indicated by fact that there is a 3D printer for public use in the town library where Al lives; anyone could theoretically print any object on a public 3D printer so security issues become even more important.
   - Continue efforts to merge the activities of the PWG IPP WG with the activities of the IDS WG so that instead of separate “stovepipes” for each WG they are an integrated part of PWG-wide activities. This involves looking more closely into the security aspects of IPP standards that the IPP WG are creating,
   - Finally, try to continue development of the HCD Security Guideline. Ira has no been able to make any headway on these guidelines since Feb 2022, so the IDS WG should look into ways it can help Ira complete the document.
5. **Actions:** None

Next Steps

- The next IDS WG Meeting will be January 26, 2023 at 3:00P ET / 12:00N PT. Main topics will be a special topic (likely the EU Artificial Intelligence Act) and a discussion on what IDS should do in 2023.
- The next PWG Face to Face Meetings will be February 7-9, 2023. The IDS WG Session will be on February 9th from 10A – 12N ET.