DHS SCIENCE AND TECHNOLOGY

Cyber Resilience Lessons Learned

Homeland Security
Science and Technology

March 26, 2019

Pat Kastner

Acting Deputy Director, National Preparedness Programs

Office of Test and Evaluation

Science and Technology Directorate

National Security Cutter (NSC) Cyber

- Cooperative Vulnerability Penetration Assessment conducted from 26 February through 20 March 2018

- Adversarial Assessment (AA)

  conducted 14 through 29 August 2018

- System Restoration:
  - Began 29 August 2018 and paused on 07 September 2018 for Hurricane Florence Avoidance
  - Re-started on 19 September 2018 and completed on 04 October 2018

Cyber Resilience COI

- Does NSC cyber resilience protect, detect, react and restore capabilities to protect mission-critical data, prevent adversary access and support mission completion in a cyber-contested environment?

Protect, Detect, React and Restore

Cyber Table Top

- CTTs, do them early, do them often
- For complex platforms or systems with lots of interoperability consider holding the CTT over multiple sessions with each one focused on enclaves of similar sub-systems (for a ship the enclaves would be Combat systems, propulsion, C2, admin, etc.)
- First level CTT could be done at the EOA just to identify enclaves and proposed subcomponents (network/server types, PLCs, etc.)

Test Planning

- If testing on an actual system (not a lab version), develop an emergency restoration plan to quickly restore essential functionality in event of contingencies (e.g., hurricanes)

- Establish safety boundaries and limitations to test to prevent MISHAPs (e.g., don't cyber test the UAV while it is flying).

System Restoration

- Build restoration into the test plan and test period in order to better evaluate users/watchstanders
- Restoration is a sub-part of the Recovery tenant of Cyber
  - Prevent, Mitigate, Recover (PMR), DOD
- Restoration should be planned for as part of the Cyber Test, not just the clean-up following Cyber Testing
- Cyber Test Team (-) should remain on scene to both evaluate Restoration Times as well as determine if the Restoration Efforts are effective in preventing the attack again via the same vector

Questions?

Protect, Detect, React and Restore