WORKBOOK 7.1: EVALUATING CYBERSECURITY

Purpose: To provide questions that will help discuss cybersecurity with information technology managers

The following questions will help you discuss cybersecurity with your agency's information technology managers to help them evaluate the cybersecurity for critical infrastructure information systems — does your agency or organization:

- **Use a security technique that limits what programs can run at one time?**
  - **Application whitelisting:** a proactive security technique where only a limited set of approved programs are allowed to run, while all other programs (including most malicious software) are blocked from running by default; enables only the administrators, not the users, to decide which programs are allowed to run
  - This technique is different from most standard operating systems that allow all users to download and run any program they choose — including programs that have hidden malicious software that might be new and not caught by antivirus programs
  - This technique should not be used alone, but should be part of a defense-in-depth strategy which includes antivirus software and firewalls
- **Ensure that all program downloads and upgrades come from verified sources?**
  - Hostile intruders often target out-of-date software on computers — knowing where the program vulnerabilities are and then exploiting them to enter the computer
  - Information technology department best practice is to have a management program established that monitors all authorized upgrades for authorized programs and where these upgrades should come from — upgrades from all other locations are blocked
  - Computer and laptop users should not be allowed to download programs and upgrades without permission from information technology department
- **Isolate networks from any untrusted networks, especially the Internet?**
  - If there is a defined business requirement to access external networks, minimize connectivity time
  - Monitor the functions performed during connectivity
- **Separate its computer system into distinct parts?**
  - Each section is contained and thus more easily defendable so that a breach in one part will not allow access to another part
  - Communication paths between sections should be restricted
  - Normal communication can continue but unauthorized access can be stopped
  - Possible damage from an intrusion can more easily be limited
  - Intrusion incident cleanup can be significantly less costly for one section instead of the whole system
- **Have a strict policy for issuing and authenticating access credentials to the system?**
  - Hostile intruders have begun focusing on getting control of legitimate access credentials, especially those associated with highly privileged accounts, to be able to masquerade as legitimate users

  - If the system thinks a legitimate user is accessing the system, no alerts will be generated to warn of an intrusion and no evidence of the intrusion will exist
  - User privileges should be reduced to access to only those programs needed for the user's duties
  - Implement the use of secure password policies that emphasize length over complexity, stipulate unique credentials for each program, and require password changes at least every ninety days
  - Keep all credentialing information in separate systems from where they are used
- **Control remote access with strong credentials and time limits?**
  - If access to a system is allowed away from the critical infrastructure site, review its use and users and severely limit such access — this includes modems used for facsimile transmissions which are very insecure
  - Use two types of credentials where possible, such as strong passwords and tokens or strong passwords and security questions
  - Place limitations on number of access events and time of access for remaining users — lock out any user immediately that exceeds number and time limits—and change to a primarily monitoring only access format (more secure than read-only)
- **Monitor the system continuously and respond immediately to intrusion incidents?**
  - Defending the computer systems of critical infrastructure requires actively monitoring for hostile intrusions and quickly executing a prepared response
  - Monitoring should take place in the areas of abnormal or suspicious communications, malicious content, intrusion attempts, login analysis (time and place, for example, to detect stolen credential use or improper access from an unusual location, then verify with a phone call to the authorized user), and user attempts to change control settings
  - Ensure that response plans are in place so that an immediate response can be initiated if a verified intrusion is detected — examples of responses include disconnecting all Internet connections, disabling user accounts, isolating suspected systems even further, searching for intrusive programs, and implementing an immediate 100 percent password reset across the organization