Agency Cybersecurity Issue Reporting Checklist

Purpose

This checklist provides a quick reference for submitting a ticket when a user suspects or discovers a possible security incident. Providing sufficient information can expedite the response. Information required for the ticket is detailed below in the section titled **How to Report**.

Typical Symptoms

Some specific behaviors that indicate your system may be infected or compromised include:

- Downloaded or opened a potentially malicious attachment through email, or opened a link sent in a suspicious email
- Reports from coworkers or friends who received questionable emails or messages
- Receiving multiple advertising pop-up windows or virus alerts even when not browsing the Internet
- Receiving a legitimate quarantine or message from the system antivirus software (McAfee Endpoint Protection), or notification that the McAfee software is disabled
- Browser being redirected to sites that you did not select or intended to select; spontaneous change of the default home page, or unrequested installation of browser tools
- Data or files that are accessed are encrypted or corrupted, or a window appears indicating the system has been encrypted
- Computer runs very slowly and the network team or service desk has not indicated any outage or ongoing service issues
- Frequent system crashes, unusual error messages, or little to no hard drive space remaining

How to Report

If any suspicious behavior, such as the criteria described above, are observed then leave the computer as is – *avoid any actions that may change the state of the machine, including clicking on any prompts, attempting to close any windows, or shutting down or rebooting the computer*.

Instead, contact the DoIT Service Desk or the DoIT Security Operations Center (contact information listed below), and provide the following information for the service ticket:

- Identify and provide contact information of reporting user
  - □ Name
  - □ Role
  - □ Organization
  - □ Email Address
  - □ Phone Number
  - □ Physical Location
- Identify the type and configuration of the impacted system
  - □ Type (and model) of affected system
  - □ If device contains confidential data (e.g., health records or agency sensitive data)
  - □ Other potentially relevant data
- Describe the security issue
  - □ Time and location of security issue
  - □ Behavior or problem experienced

Contact Information

DoIT Service Desk: 7am to 9pm M-F
Phone: 410.697.9700
Email: service.desk@maryland.gov

DoIT Security Operations Center: 24x7
Phone: 443.713.4432
Email: soc.doit@maryland.gov