

## OD/EO/OIT Standard Operating Procedures for Malicious Code Attacks, Intrusions, and Offensive Emails

### 1. Viruses

Viruses are most commonly introduced through email, but they can be introduced through CDs or other removable media.

If a virus is found on desktop(s):

Security Team	<ul style="list-style-type: none"> <li>Notify OD IRT either via Remedy ticket or e-mail (include all relevant details)</li> </ul>
OD Incident Response Team (IRT)	<ul style="list-style-type: none"> <li>Clean the affected desktop(s)</li> <li>Report via e-mail to ISSO/Security Team               <ul style="list-style-type: none"> <li>➤ what happened</li> <li>➤ how it was fixed</li> <li>➤ if anyone else was found compromised.</li> </ul> </li> </ul> <p>Note: For widespread desktop problems, the Desktop Team will provide login scripts, if needed</p>
OD ISSO	<ul style="list-style-type: none"> <li>Prepare a note to users</li> <li>Log the incident in the incident tracker log</li> <li>If it is a major crisis, notify CRM to activate phone tree.</li> </ul>

If a virus/worm is found on a server:

OD ISSO	<ul style="list-style-type: none"> <li>Notify OIT Director and all teams to meet to participate in solution, if it is a major crisis.</li> <li>Record incident in the OD Incident Tracker Log</li> </ul>
OD ISSO	<ul style="list-style-type: none"> <li>Notify team(s) of interest to meet to participate in solution if it is <i>not</i> a major crisis</li> <li>Record incident in the OD Incident Tracker Log</li> </ul>
OD IRT, Network Operations Team, Web Development Team, and/or OD Server Administrators	<ul style="list-style-type: none"> <li>Pull plug to port if necessary (have hardcopy of cabling in case network unavailable)</li> <li>Scan servers</li> <li>Clean servers</li> <li>Re-install files</li> <li>Report findings and status to Security Team until problem is completely resolved.</li> <li>Update the Remedy ticket</li> </ul>
OD ISSO	<ul style="list-style-type: none"> <li>Report findings, status, and conclusion to CIT IRT</li> </ul>

## 2. Sara Scans

Sara Scans are proactive scans run by CIT to check all systems for vulnerabilities. CIT sends the results of these scans to OD monthly.

Security Team	<ul style="list-style-type: none"><li>• Notify OIT Teams and OD system administrators responsible for equipment shown to have vulnerabilities via email <b>within three business days</b>.</li></ul>
OIT Teams and OD System Administrators	<ul style="list-style-type: none"><li>• Report to Security Team via email <b>within three business days</b>:</li></ul>
OD ISSO	<ul style="list-style-type: none"><li>• Report findings, status, and conclusion to IRT <b>ASAP and definitely within 30 days</b>.</li><li>• Record all findings in the OD Information Assurance Vulnerability Assessment (IAVA) tracking log</li></ul>

## 3. Possible Hacker Intrusion Incidents:

Possible Hacker Intrusion Incidents are usually reported by CIT's Intrusion Detection System, e.g., pre-attack probes, unauthorized access attempts, denial of service attempts, or vulnerabilities identified as a result of a SARA scan. This could also include notification by an outside source that they are being attacked from an NIH IP address.

Security Team	<ul style="list-style-type: none"><li>• Notify all OD system administrators and the OIT Teams responsible for equipment shown to have vulnerabilities.</li></ul>
OIT Teams and OD System Administrators	<ul style="list-style-type: none"><li>• Look at the type of warning</li><li>• Check the logs unless you are certain that the system is not vulnerable, e.g., previous patch.</li><li>• If successful intrusion is noted, proceed to part 4, Active Hacker Incidents, below.</li><li>• Report findings to the OD ISSO</li></ul>
OD ISSO	<ul style="list-style-type: none"><li>• Report findings to CIT</li><li>• Record findings in OD IAVA tracking log</li></ul>

## 4. Active Hacker Incidents

Active Hacker Incidents are reported by CIT's Intrusion Detection System and administrators of hacked web pages. They include confirmed unauthorized access, denial of service, and successful exploits of vulnerabilities. If there is damage being inflicted on other systems (e.g., denial of service attacks or corruption of data), web defacing, or a known root compromise, the compromise should be considered critical.

Security Team	<ul style="list-style-type: none"> <li>• Notify OIT Teams and OD Administrators</li> </ul>
OIT Teams and OD System Administrators	<ul style="list-style-type: none"> <li>• Provide daily status reports and final report to the Security Team.</li> </ul>
OD ISSO	<ul style="list-style-type: none"> <li>• Respond to CIT.</li> <li>• Note: If at any time in this process, the compromise is determined to be critical, the system should also be blocked at the firewall. Call the IRT Hotline 301-881-9726 to request the block. (ISSO/Security Team Action).</li> <li>• Request that the IRT re-run a SARA scan to be certain that no remaining vulnerabilities exist.</li> <li>• Ensure that IRT is aware of the incident status within 30 days.</li> <li>• Record all findings in the IAVA tracking log</li> </ul>

### 5. Inappropriate E-mail

OD Staff	<ul style="list-style-type: none"> <li>• Forward inappropriate e-mail message to the OD ISSO and OD CIO.</li> </ul>
OD ISSO and OD CIO	<ul style="list-style-type: none"> <li>• Determine the level of inappropriateness</li> <li>• Forward the message to the appropriate NIH official at CIT and/or ORS Division of Public Safety.</li> </ul>