

Implementing the OIS Security Vulnerability Reporting and Response Guidelines, Version 2.0

Purpose

Many people and organizations have expressed an interest in implementing the process described in the Organization for Internet Safety's publication, *Guidelines for Security Vulnerability Reporting and Response V2.0* (<http://www.oisafety.org/guidelines/secresp.htm>). The OIS has prepared this document to assist potential adopters in identifying tasks that need to be completed to deploy a security reporting or response process that complies with the Guidelines.

This paper discusses policy decisions, publications, and infrastructures that need to be completed to support the processes. It assumes that the adopter already has a basic infrastructure in place, including telephone, email service, and a web presence, and focuses on tasks that are specifically required to implement the Guidelines. This paper does not address how the adopter will implement the processes described in the Guidelines, such as how the adopter researches the validity of the vulnerability report.

Required Tasks

To implement the Guidelines, adopters need to complete a small number of tasks. These tasks serve to document the adopter's policies and develop infrastructure that supports the security reporting or response process. The table below lists each of these requirements, whether it applies to Vendors or Finders, and the reference in the Guidelines that discusses the requirement.

Table 1. Required Tasks

Task	Applies to	Reference
Develop a security reporting and/or response policy and post it in an easily discoverable location on its web site.	Both	§1.3
Identify any provisions of the OIS Guidelines that the adopter has chosen <i>not</i> to implement, and list them in the security reporting/response policy.	Both	§1.3
Identify a single person or organization who receives vulnerability reports, and include contact information in the security response policy.	Vendor	§5.1.1 §5.1.3
Implement steps to accommodate Finders who wish to remain anonymous	Vendor	§5.1.2
Implement steps to ensure that emails misdirected to several common email addresses are re-routed to the correct security response contact.	Vendor	§5.1.5
Provide a method of securing communications with the Finder, and include instructions in the posted contact information.	Vendor	§5.1.4 §5.1.8
Develop and maintain a public listing of supported products and versions.	Vendor	§6.2.4
Be capable of localizing remedies to support localized product versions.	Vendor	§7.5.1
Provide an easily discoverable, public repository of all of the vendor's published security advisories, and include the repository location in the security response policy.	Vendor	§8.3.1 §8.3.2 §8.3.3
Provide a means by which readers can confirm the origin and authenticity of the adopter's security advisories.	Both	§8.3.5

Optional Tasks

In addition to the tasks listed above, there are other steps that adopters may wish to take before deploying a security reporting or response process. In most cases, these tasks involve activities that, if not completed beforehand, may need to be completed the first time the process is used.

Table 2. Optional Tasks

Task	Applies to	Reference
Include a list of recommended Coordinators in the security reporting/response policy.	Both	§3.2.1.3
Determine whether to use the sample communications provided in the Guidelines, or develop custom ones.	Both	§4.1.1 §5.2.1 §5.2.3 §5.2.5 §6.1.1 §6.1.3 §6.1.5
Determine, and document in the security response policy, whether the vendor will issue public notifications when receiving vulnerability reports.	Vendor	§5.3.1
Develop a policy for handling cases in which a vulnerability involves a code base shared by multiple vendors.	Both	§6.3 §7.6
Provide a means of proactively notifying interested parties when publishing new security advisories.	Vendor	§8.3.6
Develop a template for security advisories.	Both	§8.3.11 §8.3.12
Determine, and document in the security reporting/response policy, the criteria for acknowledging participant's contributions to security investigations.	Both	§8.3.12
Develop a template for documenting security fixes that are delivered as part of maintenance updates.	Vendor	§8.5