FEMA

ADDITIONAL INFORMATION

REVIEW CYCLE

FP 404-21-001, "Cyber Vulnerability Disclosure Policy for Public-Facing Systems and Services" will be reviewed, reissued, revised, and/or rescinded within four (4) years of the issue date.

AUTHORITIES AND REFERENCES

Authorities

A. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), Binding Operational Directive 20-01, "Develop and Publish a Vulnerability Disclosure Policy"
B. Office of Management and Budget (OMB) Memorandum M-20-32, "Improving Vulnerability Identification, Management, and Remediation"
C. 44 U.S.C. §§ 3552-3554, "Information Security"

Note: Policies do not have the force and effect of law, except as authorized by law or as incorporated into a contract.

References

A. CISA Coordinated Vulnerability Disclosure (CVD) Process
B. The CERT® Guide to Coordinated Vulnerability Disclosure
C. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 29147:2018, "Information Technology - Security Techniques - Vulnerability Disclosure"
D. ISO/IEC 30111:2019, "Information Technology — Security Techniques — Vulnerability Handling Processes"
E. NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations"

DEFINITIONS

Service: An information technology (IT) service is provided to one or more customers, by an IT service provider. An IT service is based on the use of IT and supports the agency's business process. An IT service consists of a combination of people, processes, and technology. Sometimes IT systems are acquired as tools for users, but most of the time, a government IT system is the backend implementation of an information service.

Social Engineering: The use of deception to manipulate individuals into divulging confidential or personal information or to act contrary to security protocols.

System: An IT system is an underlying automated technological component used to provide an IT service or services to users or other information systems/applications. In some cases, a service and system may have the same name, but most IT systems exist to deliver information or implement a service. A "system" is often simply a tool that exists to make some task easier or possible, typically utilizing Web technologies. By itself, the operation of an IT system could be a service, but it is the mission function that the system enables that is the actual service being provided.

Triage: Initial post-detection response to a suspected incident.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Such a weakness can be used by a party to cause the software to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness. Vulnerabilities are often found in individual software components, in systems comprised of multiple components, or in the interactions between components and systems. They are typically exploited to weaken the security of a system, its data, or its users, with impact to their confidentiality, integrity, or availability.

Vulnerability Disclosure: The act of initially providing vulnerability information to a party that was not believed to be previously aware. The individual or organization that performs this act is called the "reporter."

MONITORING AND EVALUATION

The Office of the Chief Information Officer will monitor implementation of this policy and completion of relevant guidance to support this policy. Lessons learned, questions, and concerns raised related to the implementation of this policy will be used to inform future revisions.

QUESTIONS

Address any questions or concerns, or report potential or discovered vulnerabilities in FEMA systems and/or services, to the FEMA Vulnerability Disclosure Team at FEMA-VDP@fema.dhs.gov.