



# NIST Computer Security Incident Handling Guide

---

Guidance Software Comments

**January 2004**

By Guidance Software

## I. Introduction

The Federal Information Security Management Act (FISMA) of 2002, which became effective in December 2002, mandates that Federal agencies **must establish incident response capabilities**.<sup>1</sup> FISMA requires that Federal agencies implement an incident response capability consistent with the guidelines and standards established by the National Institute of Standards and Technology (NIST).<sup>2</sup> Pursuant to this specific mandate under FISMA, NIST has now issued Special Publication 800-61, "Computer Security Incident Handling Guide," which sets forth detailed technical, procedural and policy guidelines for Federal agencies to implement a comprehensive incident response and computer forensics capability.

An incident response process that utilizes computer forensics represents an integrated framework for responding to computer security events throughout an agencies' wide-area-network. Computer security events range from intrusions and other network security breaches, to incidents perpetrated by insiders, such as fraud, espionage, unauthorized access to confidential data, or computer usage policy violations. With the vast majority of data now stored in digital format, computer forensics is the primary process for responding to, investigating and prosecuting these wide-ranging security events. The NIST Guidelines are notable in that they specifically recommend Federal Agencies to utilize incident response analysis processes that are forensically sound, thus enabling subsequent prosecution of perpetrators and an accurate investigation process.

Section 2.2 of the NIST Guidelines note: *"Heightened national security concerns are also raising awareness of the possible effects of computer-based attacks. These events—and many more—make the case daily for responding quickly and efficiently when computer security defenses are breached. To address these threats, the concept of computer security incident response has become widely accepted and implemented in the Federal Government, private sector, and academia.*

*The following are benefits of having an incident response capability:*

- + *Responding to incidents systematically so that the appropriate steps are taken*
- + *Helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information, and disruption of services*
- + *Using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data*
- + *Dealing properly with legal issues that may arise during incidents."*

This white paper provides a management and technical *summary* of the NIST Incident Handling guidelines, with a focus on the adaptation and implementation of the NIST technology requirements and incident response investigation procedures. The second half of the white paper addresses how the functionality of Guidance Software's EnCase Enterprise Edition software maps to nearly all of these important requirements.

## II. Challenges and Issues

The executive summary of the NIST Computer Incident Handling Guide ("NIST Guidelines") identifies and outlines several key issues and considerations regarding incident response. NIST recognizes the fundamental role that incident response has become in information security: *"Computer security incident response has become an important component of information technology (IT) programs.*

---

<sup>1</sup> 44 U.S.C. § 3544 (b)(7).

<sup>2</sup> 44 U.S.C. § 3549, incorporating and amending 40 U.S.C. § 11331.

*Security-related threats have become not only more numerous and diverse but also more damaging and disruptive.”*

It is also noted that despite best security practices, security breaches will occur: *“Preventative activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented.”*

Thus, the NIST Guidelines correctly note that: *“An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. To that end, this publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.”*

With EnCase Enterprise Edition, Guidance Software is uniquely positioned to provide a comprehensive incident response and computer forensics system that addresses the demanding requirements for incident handling as detailed by the NIST Guidelines. The remainder of this paper details the primary provisions of the NIST Guidelines with a focus of the technology requirements and the application of EnCase Enterprise Edition to thoroughly address and manage the requirements.<sup>3</sup>

### **III. NIST Incident Response Guidelines: Technical Infrastructure Requirements**

A key area of focus of the NIST Guidelines centers on the technical procedures and methodologies for incident response. The NIST Guidelines note that the Computer Incident Response Team (CIRT) will need a repertoire of hardware, network, and software tools to effectively execute incident response and forensics. Importantly, NIST calls for the tools to quickly gather static data, dynamic data, and log files without altering the data for purpose of future prosecution: *“Evidence should be collected according to procedures that meet all applicable laws and regulations, developed from previous discussions with legal staff and appropriate law enforcement agencies.”<sup>4</sup>*

#### **A. Technical Requirements for Incident Response**

Section 3 of the NIST guidelines calls for the following key technical processes and methodologies for effective incident response:

1. **Immediate response capability.** NIST comments: *“It is generally desirable to acquire evidence from a system of interest as soon as one suspects that an incident may have occurred.”*
2. **Initial System Snapshot.** In addressing this critical aspect of incident response, NIST correctly notes that: *“Many incidents cause a dynamic chain of events to occur; an initial system snapshot may do more good in identifying the problem and its source than most other actions that can be taken at this stage.”*
3. **Analyze live systems with minimal invasiveness.** The Guidelines note that without proper procedures, *“risks are associated with acquiring information from the live system. Any action performed on the host will alter the state of the machine...”*

---

<sup>3</sup> Also addressed in the NIST Guidelines are non-technical policy and organizational matters, such as the establishment of an incident response team, employee policies, and administration procedures. These policy and organizational issues are not addressed in detail in this paper.

<sup>4</sup> Section 3.3.2, at page 3-18

4. **Volatile data acquisition and analysis:** The Guidelines provide: *“...it is often desirable to capture volatile information that may not be recorded in a file system or image backup, such as current network connections, processes, login sessions, open files, network interface configurations, and the contents of memory. This data may hold clues as to the attacker’s identity or the attack methods that were used.”*
5. **Forensic hard drive data acquisition.** The NIST Guidelines provide clear direction on this issue: *“After acquiring volatile data, an incident handler with computer forensics training should immediately make a full disk image ... (which) preserves all data on the disk, including deleted files and file fragments.”*
6. **Computer forensic analysis.** Section 3.3.2 of the Guidelines state: *“Computer forensics software is valuable not only for acquiring disk images, but also for automating much of the analysis process, such as:*
  - *Identifying and recovering file fragments and hidden and deleted files and directories from any location (e.g., used space, free space, slack space)*
  - *Examining file structures, headers, and other characteristics to determine what type of data each file contains, instead of relying on file extensions (e.g., .doc, .jpg, .mp3)*
  - *Displaying the contents of all graphics files*
  - *Performing complex searches*
  - *Graphically displaying the acquired drive’s directory structure*
  - *Generating reports.”*
7. **Establish a Proper Chain of Custody with a Message Digest Hash Algorithm.**
8. **Log file acquisition and analysis.**
9. **Ability to correlate multiple time zones of acquired media.**
10. **Validated computer forensics technology via courts and independent testing,** as stated by NIST: *“Evidence should be collected according to procedures that meet all applicable laws and regulations . . . so that it should be admissible in court.”*

## **B. EnCase Enterprise Supports NIST’s Incident Response Requirements**

EnCase Enterprise provides all the functionality for effective incident response identified by NIST in the above section, in addition to many additional features and benefits. Specifically, EnCase Enterprise maps to the 10 specified incident analysis requirements from the NIST Guidelines as follows:

1. **Immediate response capability:** A key benefit of EnCase Enterprise is its revolutionary ability to conduct immediate and thorough forensic analysis of any system on a wide-area-network, without disrupting operations. Many Federal agencies have deployed EnCase Enterprise for an immediate global incident response and computer forensic capability. This immediate response capability enables organizations to better contain and mitigate incidents as they occur.
2. **Initial System Snapshot.** The Snapshot feature of EnCase Enterprise is a central feature of EnCase Enterprise specifically designed for rapid and thorough incident response analysis. A snapshot of all the key volatile and binary data is quickly obtained of any compromised system on the wide-area-network.

3. **Analyze live systems with minimal invasiveness.** Another important advantage of EnCase Enterprise is its ability to analyze live systems in a forensically sound manner without taking those systems off-line, or even being visible to the user or the attacker. While the Guidelines note that the need for a proper forensic analysis is often balanced against the operational interest of maintaining business continuity, EnCase Enterprise does not require any such compromise.
4. **Volatile data acquisition and analysis:** EnCase Enterprise supports this critical aspect of incident response by quickly obtaining and displaying all the relevant volatile data, such as open ports, open files, running processes, and the live registry. EnCase can capture and examine the volatile data from several systems at once, which is important when the exact location of the compromise needs to be determined. Additionally, EnCase Enterprise does this remotely and in a non-invasive manner, without disrupting the system being investigated.
5. **Forensic hard drive data acquisition,** EnCase is adept at obtaining complete and accurate forensic images of hard drives. EnCase has been validated and thoroughly tested by NIST in its separate computer forensics tool testing project.<sup>5</sup> EnCase can create these images on a local drive or, with EnCase Enterprise, of any computer on a wide-area-network.
6. **Computer forensic analysis.** In addition to disk imaging, EnCase provides industry leading computer forensics analysis capability, including all the functions listed in Section 3.3.2 of the NIST Guidelines, as well as many additional features.
7. **Establish a Proper Chain of Custody with a Message Digest Hash Algorithm.** The EnCase acquisition process features an integrated process to establish a proper chain of custody, including the secure generation of a MD5 hash for the forensic image and CRC's for every 32K of data for authentication.
8. **Log file acquisition and analysis.** Log files are maintained by various systems and appliances throughout an organization's network. EnCase supports the collection, parsing and analysis of log files. Furthermore, skilled attackers know the importance of log files and may delete them in an attempt to cover their tracks. The deleted file recovery functionality of EnCase is therefore important to quickly recover any such deleted log files.
9. **Ability to correlate multiple time zones of acquired media.** With integrated correlation tools and a timeline viewer, EnCase is specifically designed to support the analysis and correlation of dates and times originating in different time zones.
10. **Validated computer forensics technology via courts and independent testing.** EnCase is unparalleled in being specifically accepted by the courts in appellate and trial court decisions.<sup>6</sup> In addition, NIST is one of many agencies that have independently tested and validated the EnCase program.<sup>7</sup> Many IT administrative tools that are sometimes employed for incident response purposes are highly invasive and fail to establish a proper chain of custody, and thus do not meet legal requirements for the admission of any gathered evidence. It is therefore essential that Federal agencies utilize forensic technologies that meet legal requirements for the admission of computer evidence.

---

<sup>5</sup> See [www.ojp.usdoj.gov/nij/sciencetech/ecrime.htm](http://www.ojp.usdoj.gov/nij/sciencetech/ecrime.htm) for the results of the NIST Computer Forensics Tool Testing Project and Guidance Software's comments to the EnCase test report at [www.guidancesoftware.com/products/software/EnCaseForensic/NIST2003Response.pdf](http://www.guidancesoftware.com/products/software/EnCaseForensic/NIST2003Response.pdf) 5

<sup>6</sup> *State v. Cook*, 2002-Ohio-4812, 2002 WL 31045293 (Appellate court expressly validates the authenticity of an EnCase image); *Williford v. State*, 2004 WL 67560 (Tex.App.-Eastland) (EnCase validated under *Frye/Daubert* standard).

<sup>7</sup> See note 5.

## C. Additional NIST Policy Requirements Supported By Guidance Software and EnCase

In addition to the technical and procedure requirements noted above, there are three particularly important policy considerations outlined by NIST that support proper incident handling:

**1. Inter-Agency Collaboration:** As noted by the NIST Guidelines, the Office of Management and Budget (OMB) requires that agencies develop an incident response capability that enables agencies to collaborate and coordinate in cross-agency investigations and prosecutions, and share information to strengthen defenses against common threats. In directly addressing this important OMB directive, the NIST Guidelines state as follows:

*“Besides the business reasons to establish an incident response capability, Federal departments and agencies must comply with law, regulations and policy directing a coordinated, effective defense against information security threats. Chief among these are the following:*

*+ OMB’s Circular No. A-130, Appendix III,<sup>8</sup> which directs Federal agencies to “ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations ... and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.”*

*+ FISMA, which requires agencies to have “procedures for detecting, reporting, and responding to security incidents” and establishes a centralized Federal information security incident center, in part to:*

- “Provide timely technical assistance to operators of agency information systems ... including guidance on detecting and handling information security incidents ...*
- Compile and analyze information about incidents that threaten information security ...*
- Inform operators of agency information systems about current and potential information security threats, and vulnerabilities ...”<sup>9</sup>*

Additionally, in its May 16, 2003 FY 2002 Report to Congress on Federal Government Information Security Reform, the OMB states that it is working closely with the Department of Homeland Security to “improve the Federal Government’s response to cyber attacks.” The OMB notes that “the integration of FedCIRC, the National Infrastructure Protection Center (NIPC), the National Communications System, (NCS), and the CIAO under the Information Analysis and Infrastructure Directorate of DHS . . . presents an opportunity for the Administration to strengthen government-wide processes for intrusion detection and response.”<sup>10</sup>

EnCase Forensic Edition is utilized by over fifty different Federal agencies, including all federal law enforcement computer crime units, while EnCase Enterprise Edition (network-enabled computer forensics and incident response) is currently employed in over a dozen Federal agencies. Thousands of Federal agents and other federal computer professionals have received computer forensics training from Guidance Software. In addition to directly mapping to the OMB requirements of greater efficiency, centralization, and compatibility, such common usage greatly facilitates multi-agency investigations, the prosecution of the computer crimes committed within Federal networks, and intelligence and information sharing.

---

<sup>8</sup> [www.whitehouse.gov/omb/circulars/a130/a130trans4.html](http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)

<sup>9</sup> See Section 2.2 of OMB Circular No. A-130, Appendix III

<sup>10</sup> See Section V(E) of OMB FY2002 Report to Congress on Federal Government Information Security Reform

**2. Prosecution of Computer Crimes:** While many organizations in the private sector choose to not disclose and prosecute computer security incidents, such a practice is generally not acceptable for the United States Government. The NIST Guidelines note that, where feasible, Federal agencies should prosecute perpetrators, consistent with Department of Justice guidance.<sup>11</sup> This is only possible if proper computer forensics processes are utilized to preserve, authenticate, and analyze the relevant computer data. As noted above, EnCase is widely recognized by courts and the computer investigation industry as the leading computer forensics software program. Federal civilian agencies that respond to incidents with EnCase Enterprise Edition will be utilizing the same process to establish a chain of custody as federal law enforcement. In addition to ensuring proper handling of computer evidence, first responders will enable a seamless and efficient transition of investigations to federal law enforcement by providing forensic disk images, which are called EnCase Evidence Files, and their case files containing their saved work of the ongoing investigation (e.g. keyword searches, recovered evidence, noted files).

**3. Training:** The NIST Guidelines are clear in requiring that the incident response team members are properly trained in computer forensics and incident response procedures. Guidance Software has trained several thousand Federal agents and other Federal officials on computer forensics and incident response procedures. Guidance Software, which has the largest computer forensics training staff in the world, bases its training on the EnCase software, in addition to other aspects of the computer investigation process.

#### **IV. Conclusion and Summary**

By enacting FISMA, Congress has mandated that Federal agencies adopt incident response capabilities, and further directed NIST to develop guidelines for the implementation of incident response processes. NIST has now issued its guidelines in its Special Publication 800-61, Computer Incident Handling Guide.

EnCase Enterprise Edition is a very powerful incident response and computer forensics system that maps to numerous requirements and recommended practices set forth in the NIST Guidelines. No other technology solution rivals EnCase Enterprise in terms of enabling compliance with NIST Special Publication 800-61.

Several thousand professionals in the Federal government use EnCase and have been trained on the software. EnCase Enterprise Edition is specifically designed to provide on-demand enterprise-wide incident response and forensic analysis, thus enabling immediate, thorough, and non-disruptive computer forensic investigation of desktops and servers anywhere on a wide-area-network from a centralized location.

---

<sup>11</sup> See Sections 3.3.2; 3.4.3; 6.4.2