# COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

# INFORMATION TECHNOLOGY SECURITY THREAT MANAGEMENT GUIDELINE

Virginia Information Technologies Agency (VITA)

# ITRM Publication Version Control

ITRM Publication Version Control: It is the user's responsibility to ensure that he or she has the latest version of the ITRM publication. Questions should be directed to the Associate Director for Policy, Practice and Architecture (PPA) at VITA's IT Investment and Enterprise Solutions (ITIES) Directorate. ITIES will issue a Change Notice Alert when the publication is revised. The alert will be posted on the VITA Web site. An email announcement of the alert will be sent to the Agency Information Technology Resources (AITRs) at all state agencies and institutions, as well as other parties PPA considers interested in the publication's revision.

This chart contains a history of this ITRM publication's revisions:

| Version | Date | Purpose of Revision |
|---|---|---|
| Original | 07/01/2007 | Base Document |
| | | |

# Preface

### *Publication Designation*

ITRM IT Security Threat Management Guideline

**Subject**
Information Technology Threat Management

**Effective Date**
**07/01/2007**

**Scheduled Review**
One (1) year from effective date

**Authority**
*Code of Virginia* § 2.2-603(F)
(Authority of Agency Directors)

*Code of Virginia*, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO))

**Scope**
This *Guideline* is offered as guidance to all Executive Branch State agencies and institutions of higher education (collectively referred to as "agency") that manage, develop, purchase, and use information technology (IT) resources in the Commonwealth.

**Purpose**
To guide agencies in the implementation of the information technology contingency planning requirements defined by ITRM Standard SEC501-01.

**General Responsibilities**
(Italics indicate quote from the Code of Virginia)

**Chief Information Officer**
In accordance with *Code of Virginia* § 2.2-2009, the CIO is assigned the following duties: *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits."*

**Chief Information Security Officer**
The CIO has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity and availability of the Commonwealth of Virginia's IT systems and data.

**ITS Investment and Enterprise Solutions Directorate**
In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the IT Investment and Enterprise Solutions Directorate the following duties: *Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions*."

**All Executive Branch State Agencies**
In accordance with § 2.2-603, § 2.2-2005, and §2.2-2009 of the *Code of Virginia*,, all Executive Branch State Agencies are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines issued by the Chief Information Officer of the Commonwealth.

## Definitions

**Agency** All Executive Branch State agencies and institutions of higher education that manage, develop, purchase and use IT resources in the Commonwealth of Virginia (COV).

**CISO** - Chief Information Security Officer – The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures and standards to protect the confidentiality, integrity and availability of COV IT systems and data.

**Data** - Data consists of a series of facts or statements that may have been collected, stored, processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information. Information can be processed and used to draw generalized conclusions or knowledge.

**Data Communications** - Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate COVA data between and among computer systems, including the hardware, software, interfaces and protocols required for the reliable movement of this information. As used in this Guideline, Data Communications is included in the definition of government database herein.

**Data Owner** - An agency manager responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

**Intrusion Detection Systems (IDS) -** Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

**Intrusion Prevention Systems (IPS) -** Software that prevents an attack on a network or computer system. An IPS is a significant step beyond an IDS (intrusion detection system), because it stops the attack from damaging or retrieving data. Whereas an IDS passively monitors traffic by sniffing packets off a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

**ISO** – Information Security Officer - The individual who is responsible for the development, implementation, oversight and maintenance of the agency's IT security program.

**IT System** - An interconnected set of IT resources and data under the same direct management control.

**Risk** – The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

**Risk Assessment (RA)** – The process of identifying the vulnerabilities, threats, likelihood of occurrence, potential loss, or impact, and theoretical effectiveness of security measures. Results are used to evaluate the level of risk and to develop security requirements and specifications.

**Risk Management –** The continuous process of determining, prioritizing, and responding to risks.

**Risk Mitigation** – The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

**Sensitive Data -** Any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of agency programs, or the privacy to which individuals are entitled.

**Sensitive IT Systems** - COV IT systems that store, process or transmit sensitive data.

**System Owner** -An agency manager responsible for the operation and maintenance of an agency IT system.

**Threat -** Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data and/or denial of service by exploiting vulnerability.

**Threat Detection –** Programs, policies, procedures and technologies that enable organizations to identify and respond to threats.

**Vulnerability***:* A condition or weakness in security procedures, technical controls or operational processes that exposes the system to loss or harm.

**Related ITRM Policy and Standards**
ITRM Policy, SEC500-02: Information Technology Security Policy (Effective Date: 07/01/2006)
ITRM Standard SEC501-01: Information Technology Security Standard (Effective Date: 07/01/2006)
ITRM Standard SEC502-00: Information Technology Security Audit Standard (Effective Date: 07/01/2006)

## TABLE OF CONTENTS

# 1 Introduction

## 1.1 Information Technology Security

In order to provide overall Information Technology (IT) security that is cost-effective and risk based, information technology security threat management must be a part of an agency's comprehensive risk management program. This guideline presents a methodology for threat management suitable for supporting the requirements of the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Information Technology Security Policy (ITRM Policy SEC500-02), the COV ITRM Information Technology Security Standard (ITRM Standard SEC501-01), and the COV ITRM Information Technology Security Audit Standard (ITRM Standard SEC502-00). These documents are hereinafter referred to as the "Policy," "Standard," and "Audit Standard," respectively. Agencies are not required to use this guideline, and may use methodologies from other sources or develop their own methodologies, provided that the methodologies implement the requirements of the policy and the standard.

## 1.2 Information Technology Security Threat Management

Information technology security threat management combines IT security disciplines of threat detection, incident management, and monitoring and logging in order to in order to reduce the impact of risks to an organization's IT systems and data.

Many organizations provide information on new developments in threat management. These include:

- CERT (http://www.cert.org/), a center of internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.
- The SANS (SysAdmin, Audit, Network, Security) Institute (http://www.sans.org/), a cooperative security research and education organization.
- Security Focus (http://www.securityfocus.com/), a vendor-neutral site that hosts the Bugtraq mailing list, traditionally one of the first places where new vulnerabilities are discussed.[1]

[1] These hyperlinks are current as of March 2007.

# 2 IT Security Threat Detection

The goal of the threat detection process is to lower the difference in mean time between when an attack occurs and when responsible agency staff becomes aware of an issue. Threat detection is implemented through intrusion detection and protection practices.

## 2.1 Threat Detection Roles and Responsibilities

Each agency must designate an individual responsible for the agency's threat detection program.

The amount of training and experience necessary to fulfill this function will vary depending on whether an agency provides its own threat detection services or depends on a service provider. Table 1 outlines the two approaches.

**Table 1 Skills Necessary for Threat Detection Program**

| Program Type | Who provides technical services | Recommended Training or Experience for Agency Staff | Responsibilities |
|---|---|---|---|
| **Internal** | agency | • Incident handling<br>• Intrusion detection<br>• Infrastructure protection<br>• Intrusion prevention<br>• Security management | Oversee agency Threat Management Program<br>• Planning<br>• Development<br>• Acquisition<br>• Implementation<br>• Testing<br>• Training<br>• Maintenance |
| **Service Provider** | service provider | • Infrastructure protection<br>• Security management | Oversee agency Threat Management Program<br>• Planning<br>• Development<br>• Training |

Specialized training in the necessary subjects is available from several sources. One source for threat detection training is the SANS GIAC (Global Information Assurance Certification) training programs (http://www.giac.org/overview/)[2].

[2] This hyperlink is current as of March 2007.

## 2.2 Threat Detection Activities

Intrusion detection and prevention technologies are significant components of an effective threat detection strategy. Data collected from intrusion detection systems (IDS) and/or intrusion protection systems (IPS) help identify events that could constitute an incident[3]. To achieve the goal of threat management, data should be monitored and correlated in as close to a real time manner as possible. IDS / IPS logs should be frequently reviewed to detect new attack patterns quickly and develop required responses.

Methods used to monitor and correlate IDS/IPS data depend on the size of the organization. A small agency or organization with few monitored assets might be successful with a simple manual review of logs by security staff once or twice a day. A large agency or organization with many monitored assets and log data streams will need an automated tool in addition to trained security staff to be effective.

## 2.3 Intrusion Detection

An IDS can be either host-based (HIDS) or network-based (NIDS). HIDS typically act as a file-integrity checking service that monitors crucial system files, directories, and configurations for changes. HIDS may also include network based IDS components.

NIDS are the primary intrusion technology in usage today. They consist of a capture engine and an analysis engine. The capture engine monitors and records all OSI Model Layer 2[4] network traffic that is seen on the physical segments to which it is attached. The capture engine forwards this recorded traffic to the analysis engine for processing.

There are two types of analysis engines. Table 2, shown on the next page to improve its legibility, outlines their differences.

[3] Incident refers to an adverse event in an information system, network, and/or workstation, or the threat of the occurrence of such an event.

[4] OSI Layer 2 traffic is network traffic at the data link layer of the seven-layer OSI Basic Reference Model as well as of the five-layer TCP/IP reference model. It responds to service requests from the network layer and issues service requests to the physical layer. This is the layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. More information about the OSI Basic Reference Model is available at:
http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm (as of March 2007).
More information about the TCP/IP model is available at:
http://www2.themanualpage.org/networks/networks_tcpip.php3 (as of March 2007).

**Table 2 Intrusion Detection Systems Type**

| Analysis Type | How Does it Analyze? | Strengths | Weaknesses |
|---|---|---|---|
| **Signature Based** | These systems take the traffic recorded by the capture engine and run an analysis against a series of signatures containing the traffic patterns and network packet details of known malicious traffic | • Flexibility of configuration – most signature-based NIDS will allow user defined signatures<br>• Ease of updating signatures – most signature-based NIDS vendors have mechanisms in place similar to anti-virus vendors to automatically update signatures on a timely basis. | • Only as good as the signatures – an attack for which no signature exists or for which the signature is outdated will not be alerted on by the NIDS<br>• Require extensive network traffic flow knowledge to configure effectively. An improperly configured signature-based NIDS can actually harm efforts by increasing the level of traffic that must be evaluated without adding additional security. |
| **Anomaly Based** | These devices use their capture engine to first monitor and create a baseline of normal network traffic flows. Any traffic that occurs outside of the normal network baseline is then alerted upon. | • Ease of initial configuration – these systems usually create their own baselines and configurations<br>• Lack of need to keep signatures current – if the network baseline traffic changes significantly in a known way then a new baseline can be created quite simply. | • Usually no flexibility is given to the user to define additional alerting traffic<br>• Malicious traffic that fits the recorded baseline activity will not be alerted on. |

## 2.4 Intrusion Prevention

Intrusion Prevention technologies build upon network intrusion detection technologies by adding a response engine to the capture and analysis engines in an IDS, in order to provide real time attack mitigation. The IPS capture engine captures all traffic above OSI Model Layer 2, and the analysis engine analyzes captured traffic for malicious activity. The response engine then takes action based on the analysis to attempt to block or stop the malicious traffic. The primary advantage of an IPS over an IDS is this ability of the response engine to take immediate action to attempt to block or stop the malicious traffic.

Table 3, on the next page, describes the two modes of IPS function.

**Table 3 Intrusion Prevention System Modes**

| Mode | How Does it Connect and Respond? | Strengths | Weaknesses |
|---|---|---|---|
| **In-Line** | This mode requires that the IPS be physically wired into the network infrastructure in between network segments, usually at an ingress/egress point. The IPS will reside on the network segment and recording and analyzing traffic until a malicious activity is detected. When the in-line response engine detects malicious activity, it will generate appropriate blocking rules and the IPS will act as a firewall to block malicious traffic immediately. | • Malicious traffic is mitigated through layer 3 firewalling technologies which are simpler in operation and more reliable than other IPS response modes.<br>• No additional network infrastructure changes/hardware is necessary to bring this functionality online.<br>• No additional impact is placed on network switching infrastructure to provide span ports on busy network segments. | • Since in-line IPS devices directly sit on the network, when incorrectly configured they can have a negative impact on network performance as a whole, even blocking non-malicious traffic.<br>• Must make sure the IPS in-line devices fail open (as opposed to most network devices which are designed to fail closed). If this is not accounted for through IPS functionality or redundancy, then an IPS failure will drop the entire network segment that it has been wired into. |
| **Tap or SPAN** | This mode of deployment is identical to those usually used for NIDS devices, and consists of using a SPAN port or network tap to mirror traffic to the IPS interface. The IPS device can respond to malicious activity by spoofing TCP RST packets from the destination devices under attack, causing a TCP Reset Attack. This will have the effect of dropping the connection. | • Ease of deployment, especially in environments where pre-existing IDS systems are being upgraded to IPS functionality.<br>• Minimal network impact upon failure. | • TCP Reset methodology is not always successful. Must be done on an individual TCP session basis and may not scale well in detecting large denial of service attacks.<br>• Provides no functionality for UDP based attacks.<br>• Network taps and span ports must have the capability to inject traffic back into the network segment that is being mirrored. |

# 3 IT Security Incident Management

IT security incident management investigates and responds to detected attacks occurring against an agency's IT assets. The goals of the incident handling process are to minimize the impact and duration of security incidents that occur in an organization's infrastructure, and to use lessons learned during this process to revise policy and procedure to prevent re-occurrence. Additional information on IT security incident management may be found in *An Introduction to Computer Security***:** *The NIST Handbook Special Publication 800-12*, Chapter 12, "Computer Security Incident Handling". (http://csrc.nist.gov/publications/nistpubs/800-12/[5])

## 3.1 IT Security Incident Management Roles and Responsibilities

The first important step in creating an incident handling program is to identify key personnel who will comprise the Computer Incident Response Team (CIRT). The team should include technical members of the team with appropriate subject-matter expertise in the systems that the CIRT is charged with protecting.

In addition, a CIRT team should include non-technical members in order to coordinate incident response from all elements of an organization. A well-formed CIRT should have members and/or contacts from an organization's human resources, legal and communications departments, as well as clear and unfettered communications with executive management.

CIRT team members should receive training in incident handling, incident detection, and forensic procedures appropriate to their roles on the CIRT. In order to enable the CIRT to perform its duties, all levels of management should support the CIRT's mission, and make clear throughout the organization that the CIRT roles of the team take priority over their normal duties in the event of an incident.

## 3.2 Incident Handling Activities

### 3.2.1 Identify Controls

Identifying controls to deter and defend against cyber attacks, especially new forms of cyber attacks is beyond the scope of this guideline. Agencies must perform a Business Impact Analysis (BIA) and Risk Assessments (RAs) to identify potential vulnerabilities in their infrastructure that need mitigating controls, and are encouraged to work with their security engineers or service provider to plan and implement controls to mitigate risks.

### 3.2.2 Resource Prioritization

Based on the requirements identified in the BIA, agencies must develop priorities for the recovery of information resources. These priorities will guide an organization's incident response strategy. Information from critical systems will receive a more direct and focused

[5] This hyperlink is current as of March 2007.

response as compared, for example, to information stored for future month's office supplies. For critical resources, an organization requires the ability to react to and recover from security incidents as they arise, with a swift, coordinated, and effective response, which will minimize the cost and damage to the organizational infrastructure as well as to its image as perceived by the user community.

### 3.2.3 Incident Categorization

In addition to documenting recovery priorities in case of an incident, agencies must develop incident categories. Agencies should then use these categories to develop incident response strategies in advance of the occurrence of an incident.

Possible categories of security incidents include:

- Virus attacks (Unable to clean, rename, or delete)
- Denial of service attack(s)
- IDS and IPS alert notification(s) (false positives possible)
- Automated scanning tools and probes
- Internal threats (espionage)
- Unauthorized accesses to information systems

### 3.2.4 Determine Response Activities

Based on recovery priorities and incident types, the CIRT must develop procedures to respond to particular types of incidents. Each type of incident needs to be clearly defined in order to enable members to react quickly and effectively. Procedures must detail the steps to be taken by team members when alerted of an incident of a particular type. Included within the procedures must be clearly defined criteria regarding investigative goals to be achieved before an incident can be closed. The team should also include contact information of key personnel to be notified of the incident, including the:

- CIRT members;
- System owner;
- Data owner(s); and
- Information Security Officer.

Possible responses to the examples listed in Section 3.2.2 include:

- Virus attacks (Unable to clean, rename, or delete) – remove affected machines from network and restage
- Denial of service attack(s) – implement router or firewall changes to mitigate, require assistance from upstream network provider
- IDS or IPS alert notification(s) (false positives possible) – open ticket for further investigation
- Automated scanning tools and probes – ignore if from external sources and unsuccessful
- Internal threats (espionage) – contact HR and Legal, begin monitoring of user's traffic

- Unauthorized accesses to information systems – contact HR, remove or suspend user's access to system

Incident response procedures should include documentation of whether the agency's primary goal in the event of an incident is to recover from the incident as quickly as possible or to safeguard evidence of the incident in order to prosecute individuals who instigated the incident. Achieving both of these goals simultaneously is often impossible.

### 3.2.5 Establish Reporting Process

All agencies must report information security incidents to VITA within 24 hours of when the agency discovered or should have discovered their occurrence[6]. Agencies are strongly encouraged to use the guidance and forms found at http://www.vita.virginia.gov/security/incident/guidance.cfm[7] to fulfill these requirements.

### 3.2.6 Establish Agency IT Security Incident Recording and Reporting Requirements

An agency should establish internal requirements for incident notification. These should detail how a detected incident is escalated throughout the organization beyond the CIRT, and how impacted system owners and data owners are notified of the incident. These types of procedures should be fairly generic in order to map to as many types of incidents as possible.

Attachment I is an example of such a procedure. Attachment B of the procedure is a template used for incident reporting purposes. A copy of the template is also available at the website listed above, http://www.vita.virginia.gov/security/incident/guidance.cfm[8].

### 3.2.7 Establish Evidence Collection and Forensic Procedures

Depending on the type of incident, careful consideration should be given to the collection and analysis of any data that may be relevant to the incident. The CIRT should develop procedures that clearly state the types of evidence to collect when an incident occurs. These should include items such as forensic checklists, collection and preservation of evidence, and investigative procedures.

The types of evidence collected during an investigation will vary depending of the type of incident being investigated. CIRT members should receive professional training in the protection of evidence (files, system logs, and backup tapes) in case such evidence needs to be used in a court of law. This training, while discussing general rules of evidence handling, should emphasize what *not* to do; i.e., what aspects of investigation and collection to leave to teams or

[6] These requirements are contained in § 2.2-603(F) of the *Code of Virginia* (hyperlink current as of March 2007).
[7] This hyperlink is current as of March 2007.
[8] This hyperlink is current as of March 2007.

agencies with specialized forensic training and experience as well as, in some instances, legal investigative authority.

Attachment II is an example of such procedures. It includes sample forensic checklists and chain of evidence forms.

### 3.2.8 Establish Specialized Incident Response Training

Agency systems or network administration personnel should receive basic incident awareness training. Specific items which should be covered include:

- How to recognize an incident from anomalous behaviors
- Initial response procedures
- The reporting procedure and chain of escalation
- Duties and roles in providing assistance to the CIRT in investigations of systems under their control

### 3.2.9 Maintain Confidentiality of IT Security Incident Reports

Agencies should strive to maintain the confidentiality of IT security incident reports, and should not use a communications channel that may have been compromised by the incident to transmit these reports. For example, if an email system has been compromised, reports of the incident should not be transmitted via that email system. Likewise, if a network is suspected to have been compromised, incident reports should not be transmitted over that network. Maintaining this required confidentiality may require reporting the incident via another email system or network that is known to be uncompromised, or by making the initial reports of the incident via phone or fax.

# 4 IT Security Logging and Monitoring

The purpose of IT security logging and monitoring is to capture data regarding events that appear innocent in isolation, but when viewed as part of a pattern can be determined to be malicious. Firewalls and IDS/IPS devices are tools to block and record improper and malicious traffic. But neither technology is designed to have the ability to control or monitor traffic that follows normal network policies but is actually malicious in nature. In addition, multiple events often must be correlated through logging and monitoring to determine that an incident has occurred or is in progress.

For example, an agency with an internet presence will register high amounts of scans and exploit attempts on their internet-facing devices. This agency may register thousands of exploit attempts in a single day which result in no incidents. But a single exploit attempt in an IDS log, when correlated by IT security monitoring and logging with a corresponding log event of successful root or administrator login can enable an IT security engineer to determine that an incident has occurred.

## 4.1 IT Security Logging and Monitoring Roles and Responsibilities

Agencies should designate individuals responsible for the establishing and reviewing of system logs. In order to maintain adequate separation of duties, system or network administrators should not be responsible for establishing or reviewing logs for the systems under their control.

### 4.2 IT Security Logging and Monitoring Activities

#### 4.2.1 IT System Logging and Monitoring Design

There are two factors to balance when designing enterprise logging and monitoring. The first is the scope of the design, based on which devices are most important to the security posture of the agency. The second is to determine the depth to which logging and monitoring will occur, based on what logging details on those devices are important to threat detection.

Depending on agency requirements the scope of logging might vary from every device to only firewalls and core routers. Using an individual Microsoft Windows-based server as an example of depth, an agency might choose to log all security, application, and system events, or might be satisfied with logging and monitoring only failed logins.

A common error in security logging design is to provide all manner of logging facilities on core servers, but to leave the log data on the servers themselves. This is especially evident in Microsoft Windows-based environments due to Microsoft’s lack of a robust enterprise logging system – event logs are local only and overwritten at the designated size threshold. The importance of centralization is two-fold.

First and most importantly it removes log data from the control of individual server administrators. It does no good to record failed login attempts if the first thing an attacker will do upon gaining control of the system is to remove them.

Second, it gathers data from disparate systems across the enterprise into a centralized repository for analysis. It is much simpler and more efficient for a log analysis tool to analyze one centralized log from the entire enterprise, despite the larger size, than to individually visit each logging device and analyze locally.

#### 4.2.2 Event Log Monitoring and Correlation.

How log data is monitored and correlated is dependent on the size and complexity of the organization. A small agency or organization with few monitored assets might be successful with a simple manual review of logs by security staff once or twice a day. A large agency or organization with many monitored assets and log data streams will almost certainly need an automated tool in addition to security staff to be effective.

The primary category of correlation tools are security information management (SIM) tools. All SIM tools correlate log and alert data from a variety of sources and find attack patterns in the data. While the inner mechanism of these tools might vary, they are all designed to take multiple data sets, correlate related events and present a single event notification with correlated information. This correlation assists in providing a holistic view of the organization's technical IT security posture. An alert is no longer "200 open sessions on port 23 on the firewall" and "200 failed logins on Unix server" but rather "attempted brute force attack on telnet service."

The correlation of raw data from different systems will enable the agency to identify different types and trends of attack tools used by hackers for reconnaissance purposes. Data mining tools are often included in a SIM and can be used to collect raw information from a variety of systems and telecommunication devices (switches, routers, firewalls and gateways) across the agency.

# 5 Appendices

These appendices provide examples and templates that agencies may use to document their use of many of the methodologies described in this guideline. Each template consists of:

1) An example of the document, completed with fictional information; and

2) A blank version of the template for use by COV agencies.

The examples use different fonts for instructions and example information, as follows:

- Times New Roman text is used for the template itself.
- **Shaded Arial Bold text** is example text.
- *Times New Roman Italic text* is provided as instructions for completing the template.

# Appendix 1 - Recording and Reporting Procedure

PURPOSE: To establish and document the notification procedure needed to report computer security incidents such as: virus/worm outbreaks, web page hacking, unauthorized intrusions, or threats to computer systems or networks, as well as security incidents including: wireless access, cell phones, personal digital assistants (PDAs), fax machines, voice mail, voice systems (VOIP) and laptops.

SCOPE: All agency employees

STATEMENT OF PROCEDURE: Notification of a security incident

Any suspected event to include but not limited to a virus/worm affecting multiple systems, unauthorized intrusion or damage to a Web site or page, or unauthorized intrusion into a computer system or network or other threats to include: wireless access, cell phones, personal digital assistants, laptops, fax machines, voice mail, and voice systems should be reported immediately to the VITA Customer Care Center (VCCC) ***(see Attachment A for guidance)***. In the case of a Web site, suspect URLs must be provided to help desk. If the reporting individual is also the systems engineer for the system(s) in question, proceed directly to step 3.

The help desk will determine support staff for the systems involved and immediately contact the appropriate system engineer if necessary.

The systems engineer will verify that the incident is a security incident ***(see Attachment A for guidance)*** using the least intrusive measures and will immediately confirm the incident with the VCCC, submit an incident report via web based form (if possible) and notify their supervisor. The system engineer and responding staff should avoid additional action until contacted by a member of the Computer Incident Response Team (CIRT) unless immediate danger is posed to Commonwealth resources.

Upon receipt of incident report the CIRT will be activated. Upon confirmation of an incident other authorities may be contacted as appropriate.

Once the responding system engineer or staff is contacted by the CIRT, control of the incident passes to the CIRT. The system engineer and responding staff will continue to provide needed assistance to the CIRT for the duration of the incident.

Once the CIRT has verified the incident, the notified Supervisor will alert the appropriate COV personnel or outside authorities. For VITA Central incidents, the appropriate parties are the associate director or branch manager. For incidents on site at an agency, the appropriate parties are the ISO and AITR. The CIRT will notify VITA executive management following the CIRT's internal procedures.

The appropriate director of the affected service and the Computer Services Director will be notified by the supervisor or SLD. The appropriate supervisor or SLD will notify the owner of the affected system.

Code of Virginia, §2.2-2005, et seq.

(Powers and duties of the Chief Information Officer "CIO" and Virginia Information Technologies Agency; "VITA")

Code of Virginia, §2.2-2009, et seq.

(Additional duties of the CIO relating to security of government databases)

## ATTACHMENT A - Guidance on Reporting Incidents

The purpose of this section is to provide information that may be helpful in incident reporting. Incidents will happen and the ability to quickly identify and act in a coordinated manner can lessen the impact of an incident. The incident reporting form is an important first step in handling incidents in a coordinated response.

### Definitions

**Incident:**

Incident refers to an adverse event in an information system, network, and/or workstation, or the threat of the occurrence of such an event.

**Event:**

An event is *any* observable occurrence in a system, network, and/or workstation. Although natural disasters and other non-security related disasters (power outages) are also called events, these reporting requirements are for IS security related events only. Events can many times indicate an incident is happening.

### What to Report

An "information security incident" should be reported if it resulted in either:

a. Exposure of legally protected data in Commonwealth databases, such as financial information protected by GLBA, information protected by IRS1075 or health information protected by HIPAA; or

b. Major disruption to normal agency activities carried out via Commonwealth data communications, such as network unavailability for all or significant portions of an agency due to a denial of service (DOS) attack.

Events should be reported that have a real impact on the organization. A security incident includes, but is not limited to the following events regardless of platform or computer environment:

When damage is done

Loss occurs

Malicious code is implanted

Evidence of tampering with data

Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources)

Threat or harassment via electronic medium (internal or external)

Access is achieved by the intruder

Web pages are defaced

When you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks).

Denial of service attack on the agency

Virus attacks which adversely affect servers or multiple workstations

Other incidents that could undermine confidence and trust in the Commonwealth's information technology systems

**Do not report routine probes, port scans or other common events.**

### Clues for determining a security incident

The following are clues that a security incident may be in progress, or one may have already occurred. These indicators can have legitimate explanations and be part of day-to-day operations. The key in determining whether a suspected event is a legitimate event or is actually a security incident is recognizing when things happen without an explanation, events that are contrary to policies and procedures. The key word to using these indicators is "**UNEXPLAINED**."

Unsuccessful logon attempts

Accounting/system/network logs discrepancies that are suspicious (*e.g., gaps/erasures in the accounting log in which no entries whatsoever appear; user obtains root access without going through the normal sequence necessary to obtain this access*)

"Door knob rattling" (*e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts*)

New user accounts not created by system administrators

New files or unfamiliar file names

Modifications to file lengths or dates (*especially in system executable files*)

Attempts to write to system files or changes in system files

Modification or deletion of data

Changes in file permissions

Logins into dormant accounts (*one of the best SINGLE indicators*)

A system alarm or similar indication from an intrusion detection tool

Denial of Service (DoS) (DDoS) (*e.g. inability of one or more users to login to an account; inability of customers to obtain information or services via system*)

System crashes

Abnormally slow or poor system performance

Unauthorized operation of a program or sniffer device to capture network traffic (*e.g., presence of cracking utilities*)

Unusual time of usage (*remember, more security incidents occur during non-working hours than any other time*)

Unusual usage patterns (*e.g., programs are being compiled in the account of a user who does not know how to program; use of commands/functions not normally associated with user's job*)

Physical theft and intrusion (*e.g., theft of laptop computer with critical information*)

## Attachment B – Computer Incident Reporting Form

**Use this form to report security incidents to the Chief Information Officer of the Commonwealth. If additional information is required, you will be contacted via phone or email. To assist with our initial assessment and investigation, please provide as much information as possible.**

### STATUS

□ Site under attack □ Past incident □ Repeated incidents, unresolved

### CONTACT INFORMATION

Name/Last____________________First___________________MI_____Title________________________

Organization____________________________________________________________________________

Email_________________________________________________________________________________

Phone (_____)______________________________ FAX (_____)_________________________________

Location/Site(s) involved________________________________________________________________________________

Street Address involved________________________________________________________________________________

City__________________________________________State_________________ZIP_________________

### INCIDENT DESCRIPTION

□ Denial of service □ Unauthorized access (e.g. Intrusion/Hack)

□ Website defacement

□ Malicious code (e.g. virus/worm or trojan)

□ Threat/harassment via electronic medium (includes employees)

□ Misuse of systems (internal or external, includes inappropriate use by employees)

□ Other (specify)_________________________________________________________________________________

### DATE/TIME OF INCIDENT DISCOVERY

Date________________________________________________________Time_______________________

Duration of incident_________________________________________________________________________________

How did you detect this?_________________________________________________________________________________

Has the incident been resolved?
Explain_________________________________________________________________________

### WHO ELSE HAS BEEN NOTIFIED (CHECK ALL THAT APPLY)?

□ System administrator □ Department Director/data owner □ Human Resources

□ General Counsel □ Law Enforcement (who & when) ____________________________________________

□ Other (Please Specify) ______________________________________________________________________________

## IMPACT OF INCIDENT

□ Loss/Compromise of data □ System downtime

□ Damage to systems □ Other organizations' systems affected

□ Financial loss (estimated amount: $______________________)

□ Damage to the integrity or delivery of critical goods, services or information

## SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE

□ High (defaced Web sites)□ Medium (Trojan detected) □ Low (Small virus outbreak)

□ Unknown

## SENSITIVITY OF DATA

□ High (Privacy Act violation) □ Medium (local administration) □ Low (Public materials)

□ Unknown

## IDENTIFY THE COMPUTER OPERATING SYSTEM AND ANY OTHER SOFTWARE INVOLVED (CHECK ALL THAT APPLY)

□ Unix □ OS2 □ Linux □ VAX/VMS

□ Microsoft _ XP _2000 _NT _95/98 □ Novell □ Sun OS/Solaris

□ Other Software (Specify) ______________________________________________________________________________

## WHAT STEPS HAVE YOU TAKEN TO RESPOND (CHECK ALL THAT APPLY)?

□ No action taken □ System disconnected from network

□ Restored data from backup □ Updated virus definitions & scanned hard drive

□ Log files examined (saved and secured) □ Physically secured computer □ Other (specify)

# Appendix 2 – Internal Incident Handling Procedure

PURPOSE: To document the response procedure for potential information security incidents which threaten information systems and services.

SCOPE: All agency employees

STATEMENT OF PROCEDURE:

The CIRT (Computer Incident Response Team) will act as the incident coordinator for all reported information security incidents. The incident coordinator, under the direction of the CISO and with the assistance of the responsible agency contacts, will be responsible for coordinating all aspects of the incident handling process and the incident response process. All people involved in the incident response and clean-up are responsible for providing any needed information to the incident coordinator. The CIRT must always be involved in the investigation of information security incidents and no staff should attempt incident response without prior coordination.

The following are the required general concepts and provisions:

An incident report is received by the CIRT via the CISO or the incident reporting system.

The CIRT reviews each incident report to determine if it is actually a security incident.

If it is a confirmed incident, the appropriate parties will be contacted.

If it not a confirmed incident, the information is passed on to the appropriate parties for resolution.

The CIRT working with responsible agency management and the CISO will determine if the incident requires immediate response**.**

If so, then the CIRT will activate and begin to coordinate response activities.

If not, then the agency management and CISO will coordinate appropriate response activities.

The CIRT working with responsible agency management and the CISO will determine if the incident will require an investigation.

If so, then investigative efforts are initiated.

If not, then recovery efforts are initiated.

Initiation of Recovery and Investigation

CIRT members should log initial details an activity using the CIRT initial response checklist (Attachment A). All pertinent live forensic data should be recovered from the system before disconnection from network or powering down. Attachment B details these steps on Windows based platforms. Due to the variety of commands necessary on UNIX based platforms CIRT members should log commands via a form (Attachment C). Additional network traces performed with open standards based network sniffer tools may also be required.

Preservation of Evidence if an Investigation is Required

In cases of investigations where physical evidence is collected from the scene, CIRT members should fill out a description of evidence form (Attachment D). In cases where criminal charges may be an outcome, CIRT members should also use a chain of evidence custody form (Attachment E).

CIRT members should make forensic drive images of incident related hardware and store the originals clearly marked in a locked area. All forensic drive images should be done in open standard format (dd based) to allow the widest variety of forensic tool analysis. Proprietary image formats such as those generated by EnCase should not be used.

### Identification of Problem

CIRT members should identify the root cause of the incident and the most likely vectors of attack. If recoverable malicious binaries can be removed from the system(s) then they should be put on safe media and forwarded to the appropriate anti-virus vendor contacts.

### Containment and Recovery

CIRT members should take appropriate immediate actions to contain and control the incident. This may require removal of infected machines or entire network segments from the larger agency network. It may also require blocking agency networks from access to the internet or other Commonwealth resources. CIRT members should also develop an action plan for recovery of systems harmed in an incident with assistance from agency management and the CISO to be carried out by appropriate staff. All staff should cooperate with the directives of the CIRT in a timely manner to minimize exposure time and vulnerability.

### Restoration of Functionality

After an incident has been contained and all affected systems have returned to normal operations mode the CIRT will finish the incident response by verification of proper systems behavior.

### Follow-up analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. All involved parties should meet and discuss actions that were taken and the lessons learned. Pertinent procedures should be evaluated and modified, if necessary. If applicable, a set of recommendations should be presented to the appropriate management levels.

ATTACHMENTS:

(A) Initial Response Checklist.doc

(B) Windows Forensic Checklist.doc

(C) UNIX Forensic Command Log sheet.doc

(D) Description of Evidence Form.doc

(E) Chain of Custody Form.doc

Attachment A

Incident #: ____________ Date: ____________

Initial Response Checklist

# Contact Information

Contact Information

| | |
|---|---|
| Name: | |
| Department: | |
| Telephone: | |
| Alternate Telephone: | |
| Email: | |

Individual Reporting Incident

| | |
|---|---|
| Name: | |
| Department: | |
| Telephone: | |
| Alternate Telephone: | |
| Email: | |

# Incident Detection

| | |
|---|---|
| Type of incident: | ☐ Denial of service ☐ Unauthorized access<br>☐ Virus ☐ Unauthorized use of resources<br>☐ Hoax ☐ Theft of intellectual property<br>☐ Other:_______________________________________________<br>________________________________________________________ |
| Location of incident: | Address:<br>Building:<br>Room Number: |
| Describe the physical security at the site:<br>1. Are there locks?<br>2. Alarm systems?<br>3. Who is charge of physical security at the site? | |
| How the incident was detected: | |
| Is the information concerning the incident stored in a protected, tamper-proof manner? | |

## System Details

| | |
|---|---|
| System information: | |
| Make/Model of system: | |
| Operating system: | |
| Primary system user: | |
| System admin: | |
| IP Address: | |
| Network name: | |
| Modem connection(Y/N) | |
| What critical information is contained on the system: | |

## Incident Containment

| | |
|---|---|
| Is the incident still in progress or ongoing? | |
| Are you performing network surveillance? | |
| Is the system still connected on network?<br>If so, why is it still online? If not, who authorized removal? When will it be | |

| | |
|---|---|
| placed back online? | |

Incident #:_________________ Date:______________

| | |
|---|---|
| Are there backups of the system? | |
| Who has accessed/ touched system(s) affected since the onset of the incident? | |
| Who has had physical access to the system since the incident? | |
| Who currently knows about the incident? | |
| Is there a need to keep knowledge of the incident on a "need to know" basis? | |
| Have network devices (routers, firewalls) been configured to provide additional defense against the incident? | |

# Preliminary Investigation

| | |
|---|---|
| What is the Source IP of the attack? | |
| What investigative actions have been taken? | |
| Does a forensic dupe need to be made? | |
| Does a logical backup need to be made? | |
| Who needs to be contacted? | |

Incident #:_____________ Date:_______________

Comments:

## Hypothetical example with completed forms:

In this hypothetical example, the Virginia Agency for Examples (VAE), an in-scope agency, finds one of their Web sites defaced early on a Monday morning on March 19th, 2007. The Web site is hosted on a standalone server, and contained static web pages of a non-critical nature that detailed non-sensitive agency meeting minutes.

The VAE support staff contact the ISO, who completes the incident reporting form online at https://ssl02.vita.virginia.gov/secureCompIncidentForm/threatReporting.cfm. For purposes of illustration, the .doc version of the form is below.

## COMPUTER INCIDENT REPORTING FORM

**Use this form to report security incidents to the Chief Information Officer of the Commonwealth. If additional information is required, you will be contacted via phone or email. To assist with our initial assessment and investigation, please provide as much information as possible.**

### STATUS

□ Site under attack x Past incident □ Repeated incidents, unresolved

### CONTACT INFORMATION

Name/Last__Example___________First__Iso_________MI_____Title_Agency ISO_________

Organization___Virginia Department of Examples__________________________________________

Email_____iso.example@vde.virginia.gov____________________________________________

Phone (__804)_555-1212_____________________ FAX (_____)_________________________________

Location/Site(s) involved_______Main Branch Office____________________________________________

Street Address involved______100 Main Branch St.__

_____________________________________________________________

City___Richmond______________________________State____VA__________ZIP____23219________

### INCIDENT DESCRIPTION

□ Denial of service □ Unauthorized access (e.g. Intrusion/Hack)

X Website defacement

□ Malicious code (e.g. virus/worm or trojan)

□ Threat/harassment via electronic medium (includes employees)

□ Misuse of systems (internal or external, includes inappropriate use by employees)

□ Other (specify)______________________________________________________________________________

### DATE/TIME OF INCIDENT DISCOVERY

Date_____________March 17th 2007___________________________Time_________8:30am________

Duration of
incident________Unknown_______________________________________________________________

How did you detect this?___User Comment__________________________________________________

Has the incident been resolved? Explain____No, waiting on guidance from Security__________________

### WHO ELSE HAS BEEN NOTIFIED (CHECK ALL THAT APPLY)?

X System administrator X Department Director/data owner □ Human Resources

□ General Counsel □ Law Enforcement (who & when)

_________________________________________

□ Other (Please Specify)

______________________________________________________________________________________

### IMPACT OF INCIDENT

X Loss/Compromise of data X System Downtime

□ Damage to systems □ Other organizations' systems affected

□ Financial loss (estimated amount: $______________________)

□ Damage to the integrity or delivery of critical goods, services or information

### SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE

X High (defaced Web sites) □ Medium (Trojan detected) □ Low (Small virus outbreak)

□ Unknown

### SENSITIVITY OF DATA

□ High (Privacy Act violation) □ Medium (local administration) X Low (Public materials)

□ Unknown

### IDENTIFY THE COMPUTER OPERATING SYSTEM AND ANY OTHER SOFTWARE INVOLVED (CHECK ALL THAT APPLY)

□ Unix □ OS2 □ Linux □ VAX/VMS

X Microsoft _ XP _2000 _NT _95/98 □ Novell □ Sun OS/Solaris

X Other Software (Specify) _Microsoft IIS,

______________________________________________________________________________________

### WHAT STEPS HAVE YOU TAKEN TO RESPOND (CHECK ALL THAT APPLY)?

X No action taken

□ Restored data from backup

□ Log files examined (saved and secured)

□ Other (specify)

□ System disconnected from network

□ Updated virus definitions & scanned hard drive

□ Physically secured computer

Upon receipt of the incident report, Security Services Incident Response contacts the ISO at the contact information. Incident response will tailor its activities to the situation based on several factors such as criticality of systems or possibility of legal actions. VAE management decide that the system is non-critical at this time and can be removed from the network for a period. The decision is also made to attempt to pursue legal actions against the defacers.

Incident response begins is process by filling out the sample initial incident checklist.

Some information (such as physical location data) will be filled out on site at VAE.

Incident #: __0031907_ Date: _____03/19/07

Initial Response Checklist

# Contact Information

Your Contact Information

| | |
|---|---|
| Name: | Incident Engineer |
| Department: | VITA Security Services |
| Telephone: | 804-555-1414 |
| Alternate Telephone: | |
| Email: | Incident.engineer@vita.virginia.gov |

Individual Reporting Incident

| | |
|---|---|
| Name: | Iso Example |
| Department: | Virginia Agency for Examples |
| Telephone: | 804-555-1212 |
| Alternate Telephone: | |
| Email: | Iso.example@vae.virginia.gov |

# Incident Detection

| | |
|---|---|
| Type of incident: | ☐ Denial of service X Unauthorized access<br>☐ Virus ☐ Unauthorized use of resources<br>☐ Hoax ☐ Theft of intellectual property<br>☐ Other:_______________________________________________<br>_____________________________________________________ |
| Location of incident: | Address: 100 Main Branch Street<br>Richmond VA. 23219<br>Building:<br>Room Number: 108 |

| | |
|---|---|
| Describe the physical<br>security at the site:<br>1. Are there locks?<br>2. Alarm systems?<br>3. Who is charge of Physical Security at the site? | Y<br>Y<br>Iso Example |
| How the incident was detected: | User comment |
| Is the information concerning the incident stored in a protected, tamper-proof manner? | Y |

## System Details

| | |
|---|---|
| System information: | Agency meeting minutes web site server |
| Make/Model of system: | Dell SC1425 |
| Operating system: | Windows 2000 |
| Primary system user: | Agency secretary |
| System admin: | Web Administrator for VAE |
| IP Address: | 192.168.0.230 |
| Network name: | Minutesweb |
| Modem connection(Y/N) | N |

| | |
|---|---|
| What critical information is contained on the system: | None, agency meeting minutes only. |

## Incident Containment

| | |
|---|---|
| Is the incident still in progress or ongoing? | Site still defaced. |
| Are you performing network surveillance? | No. |
| Is the system still connected on network?<br>If so, why is it still online? If not, who authorized removal? When will it be placed back online? | Still connected waiting on incident response engineers. |

Incident #:_______0031707__ Date:______03/17/07

| | |
|---|---|
| Are there backups of the system? | Y |
| Who has accessed/ touched system(s) affected since the onset of the incident? | No one. |
| Who has had physical access to the system since the incident? | No one. |
| Who currently knows about the incident? | Agency management, ISO, and VITA Security Services |

| | |
|---|---|
| Is there a need to keep knowledge of the incident on a "need to know" basis? | No. |
| Have network devices (routers, firewalls) been configured to provide additional defense against the incident? | No. |

## Preliminary Investigation

| | |
|---|---|
| What is the Source IP of the attack? | Unknown at this time. Firewall logs will be pulled. |
| What investigative actions have been taken? | Making a forensic duplicate of drives. |
| Does a forensic dupe need to be made? | Y |
| Does a logical backup need to be made? | N |
| Who needs to be contacted? | No further contact at this time. |

Incident response arrives on site to take custody of the web server in question. Before removing the server from the network or powering down the engineer uses the sample windows forensic checklist. This will allow him to capture volatile data from the machine before powering off.

Windows Forensics Checklist Incident #_____0031707

Date ____03/17/07

Investigator____Incident Engineer_____

1. Execute trusted cmd.exe _Y__

2. Record system time and date _Y__

date > date.txt

time >> date.txt

3. Determine logged on users __Y_

Psloggedon

4. Record MCA times of all files __Y_

dir /t:a /a /s /o:d c:\

5. Record open ports ___Y

netstat –an

6. Associate Applications with open ports ___Y

fport

7. Grab process listing __Y_

pslist

8. List current and recent connections _Y__

netstat, arp, nbtstat

9. Record system time and data again _Y__

10. Document commands used during initial response _Y__

doskey /history

Comments:______________________________________________________________________

________________________________________________________________________________

________________________________________________________________________________

The incident response engineer should then fill out a chain of custody form as in the example below documenting the release of the server from VAE custody to VITA Security Services.

## Chain of Custody Form

Date: 03/17/07 Case Number: 0031707

Consent Required: Y Signature of Consenting Person: Iso Example

Tag Number: VAE4115

Description: One Dell SC1425 one U server

Person receiving evidence: incident engineer Signature: incident engineer

| From: | Date: | Reason: | To: |
|---|---|---|---|
| VAE ISO | 03/17/07 | Initial Collection | Vita Incident Response |

| | | | |
|---|---|---|---|
| From: | Date: | Reason: | To: |
| From: | Date: | Reason: | To: |

Once the incident response engineer has possession of the hardware he returns to the VITA Central Office to begin making forensic copies of the drives. As he does so, he fills out the example case information form.

## Case Information

Date: 03/17/07

Case: 0031707

Location: VAE

## CPU Information

| | |
|---|---|
| Make/Model: Dell SC1425 | Memory: 512Mb |
| Serial Number: JA498236 | Processor: 2.0Ghz Celeron |

Asset Tag Number: VAE4115

Remarks:

## Hard Drives/Removable Media

Drive 0:

Type:  Seagate

Serial number:  SG7852342

Capacity: 160Gb

Remarks:

Drive 1:

Type:

Serial number:

Capacity:

Remarks:

Drive 2:

Type:

Serial number:

Capacity:

Remarks:

Drive 3:

Type:

Serial number:

Capacity:

Remarks:

## Additional Notes

At this point, with all documentation underway, the incident response engineer can generate forensic copies of the drive of the server and begin forensic investigations.

## **Attachment B -** Windows Forensics Checklist

Incident #___________

Date __________

Investigator__________________________

1. Execute trusted cmd.exe ____

2. Record system time and date ____

```
date > date.txt

time >> date.txt
```

3. Determine logged on users ____

```
psloggedon
```

4. Record MCA times of all files ____

```
dir /t:a /a /s /o:d c:\
```

5. Record open ports ____

```
netstat –an
```

6. Associate Applications with open ports ____

```
fport
```

7. Grab process listing ____

```
pslist
```

8. List current and recent connections ____

```
netstat, arp, nbtstat
```

9. Record system time and data again ____

10. Document commands used during initial response ____

```
doskey /history
```

Comments:_____________________________________________________________________________

______________________________________________________________________________________

______________________________________________________________________________________

__________________________________________________________

**Attachment C**

| Start Time | Command Line | Trusted | Un | MD5 Sum | Comments |
|---|---|---|---|---|---|
| | | | | | |

**Attachment D**

## Case Information

Date:

Case:

Location:

## CPU Information

|  |  |
|---|---|
| Make/Model: | Memory: |
| Serial number: | Processor: |
| Asset tag number: |  |
| Remarks: |  |

## Hard Drives/Removable Media

Drive 0:

Type:

Serial number:

Capacity:

Remarks:

Drive 1:

Type:

Serial number:

Capacity:

Remarks:

Drive 2:

Type:

Serial number:

Capacity:

Remarks:

Drive 3:

Type:

Serial number:

Capacity:

Remarks:

## Additional Notes

**Attachment E**

# Chain of Custody Form

Date: Case number:

Consent required: Y N Signature of consenting person:

Tag number:

Description:

Person Receiving Evidence: Signature:

| | | | |
|---|---|---|---|
| From: | Date: | Reason: | To: |
| From: | Date: | Reason: | To: |
| From: | Date: | Reason: | To: |