



Interested in learning more  
about cyber security training?

## SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

### Creating and Managing an Incident Response Team for a Large Company

Using good communication skills, clear policies, professional team members and utilizing training opportunities, a company can run a successful incident response team. CSIRTs will continue to serve as an important component in supporting the management of risk and security in the business. By utilizing these passive and active phases of a CSIRT, the business will improve its security efforts across the enterprise and protect confidentiality, integrity and availability of its information systems.

Copyright SANS Institute  
Author Retains Full Rights



AD

Creating and Managing an Incident Response Team for a  
Large Company

*GCIH Gold Certification*

Author: Timothy Proffitt, [tim@timproffitt.com](mailto:tim@timproffitt.com)

Adviser: Pedro Bueno

Accepted:

Outline

1) Incident Response Team Basics .....3  
a) Introduction .....3  
b) CSIRT Services .....3  
i) Passive Services.....3  
ii) Active Services.....5  
iii) Management Services .....7  
c) CSIRT Policies and Standards .....8  
i) Incident Response Policy .....8  
ii) Incident Response Standards and Procedures .....9  
iii) Code of Conduct.....10  
iv) Disclosure Policy.....10  
v) Evidence Handling Procedures.....14  
2) Primary Phases of the CSIRT .....16  
a) Identification.....16  
i) Triage Role .....17  
ii) Identification Tasks.....17  
b) Containment.....19  
c) Eradication.....20  
d) Recovery .....21  
e) Lessons Learned .....21  
3) CSIRT Membership.....22  
a) CSIRT Staff .....22  
b) CSIRT Training.....24  
c) Extensions of the CSIRT.....25  
4) Conclusion.....26  
5) References.....26  
Appendix A .....28

## 1) Incident Response Team Basics

### a) Introduction

The computer security incident response team's (C.S.I.R.T.) function is to react in a timely fashion, to intrusions, types of theft, denial of service attacks and many other events that have yet be to executed or considered against their company. The CSIRT will be responsible for investigating and reporting on malicious insider activity, internet spam, human resource violations and copyright infringements.

The CSIRT will typically be called into action by a notification or triggered event but can also be called into action by a discovery while performing one of many passive services. Call Centers, Help Desks, business unit liaisons, legal representatives, email notifications or anonymous forms from an Intranet will all be entry points into calling the CSIRT into action.

### b) CSIRT Services

CSIRT serve several purposes. In addition to identifying, containing and eradicating a successful intrusion, the CSIRT will educate, communicate, execute vulnerability assessment, shape policy and more.

### i) Passive Services

There are several passive services that the CSIRT will perform to provide the company aid protecting its information systems in anticipation of future malicious activity.

### Vulnerability Assessment

The CSIRT will perform vulnerability assessment against company assets. The CSIRT will verify reported vulnerabilities and how they can be exploited. The vulnerability assessment service can help the business to identify infrastructure that is a high risk and can also provide data on a system that has had incident response procedures executed against it. The vulnerability assessment service will help identify when the recovery phase of an incident response effort has mitigated the intrusion. Maintaining current vulnerability assessment data for the company's high risk systems can better mitigate the security threats to the company.

### Announcements and Information Disclosure

The announcement function is used to notify business units of potential threats to information systems, external virus outbreaks that can affect the infrastructure and new compliance objectives. The CSIRT will monitor technical developments and trends to help identify attack vectors. The announcement service will provide guidance to the business to aid in mitigating security threats before they happen.

In some cases, when investigating an intrusion, a disclosure of sensitive information will be uncovered. In the case of medical information (ePHI) or identity theft data loss, the CSIRT will perform defined disclosure procedures. Depending on what data was exposed and which state the personally identifiable information owner resides in, the disclosure notification procedures will vary. Disclosure procedures will involve crafting notification letters, obtaining identity theft protection services for the effected parties, working with corporate communications to deal with the media, and potentially providing law enforcement evidence of the intrusion.

### Intrusion Detection Service

The intrusion detection service is conducted by the monitoring efforts of the CSIRT. In some cases the security group and the CSIRT will be separate teams and monitoring of IDS and IPS technologies may be shared. In these cases, alerting on intrusion information will be passed up to the CSIRT for incident handling. The intrusion detection service typically monitors intrusion detection equipment, intrusion prevention equipment, security event manager logs and performs periodic intrusion discovery procedures. When an event of interest is identified, the CSIRT will move into its active services mode.

### ii) Active Services

There are several services that the CSIRT will perform during an incident. The active services are typically what is expected of a CSIRT and are designed to contain, eradicate, recover, and report on an incident.

### Incident Handling

Incident handling involves analyzing the incidents and events. Incident handling's goal is to identify the scope of the incident, document the damage caused, and provide available response tactics. Incident handling typically involves incident analysis, evidence collection, tracking the origins of the intruder, response support for the victim(s) of the attack and coordination among other IRT, administrators and service providers.

### Vulnerability Handling

Vulnerability handling involves gathering data around operating system and application vulnerabilities. The CSIRT will perform assessments against hardware and software to verify suspected vulnerabilities and help determine how the vulnerabilities can be exploited. The service will aid in determining the proper response to repair a vulnerability and can notify others about the mitigating strategy.

### Evidence Handling

Evidence can be defined as any object found on an information system that could be involved in attacking the system or other systems around it. These can be computer viruses but also include exploit scripts, toolkits, log files, or even hardware devices such as physical key loggers.

## Lessons Learned Reporting

The reporting service primary goal is to document what happened and how the business can improve its' defenses. The CSIRT will conduct a "lessons learned" or a post mortem meeting to discuss the incident and educate the management team. Incident Reporting is beginning to become an auditable event for external auditors to test against.

### iii) Management Services

#### Awareness Training

Awareness training can be a service offered by the CSIRT. Since the CSIRT is typically conducting in depth investigations and vulnerability assessments against the businesses information assets, then next logical step is for the CSIRT to educate the technology teams about good security practices pertaining to the information systems that are being administered.

CSIRT will also seek opportunities to build awareness of the user base through newsletters, announcements, lessons learned, marketing campaigns, and websites.

#### Risk Assessments

The CSIRT can have important insight into risk assessments. When the business conducts a risk assessment to bring on a new technology or application, a member of the CSIRT should be a participant in the effort. The experience of the CSIRT members will help identify risk points, potential vulnerabilities, and threats.

Tim Proffitt  
- 7 -



## Compliance Certifications

The CSIRT can also perform compliance certifications. The team can conduct security evaluations on information systems or services to ensure the security or the pass / fail of a compliance regulation. The team can be used to provide guidance on best practices and recommendations for purchasing, installing or securing new systems.

### c) CSIRT Policies and Standards

Policies are documented principles adopted by the management team. The policies of an organization should be clearly understood by the entire workforce and the knowledge of the incident response policy will allow the CSIRT to act on their responsibilities.

#### i) Incident Response Policy

Building an incident response policy involves several objectives.

First, an Incident Response Policy cannot be enforced unless it has management approval. Endorsement by management is critical. Without this approval the team will be destined to encounter business road blocks that will hinder a timely incident response. In some cases, it may not even be allowed.

Second, the policy must be clear. Any employee should be able to easily understand what the policy is about. If a non-technology oriented employee is confused by the policy, then the policy should be rewritten.

Third, the policy must be to the point. A long winded policy will either be a bad policy or one that would include sections that should be in a procedure document instead.

Forth, the policy must be usable and implementable. Avoid statements that sound appropriate but will be open to interpretation. At the same time, the policy should not include objectives that the CSIRT will not be able to execute due to business processes or corporate culture.

Once the policy has been created, it is important to make regular checks against its effect on the workforce. When changes occur in the business direction or new technology systems are implemented, update the policy to match the new processes.

## ii) Incident Response Standards and Procedures

A successful CSIRT is a team that has documented standards and procedures. Standards should be written from how the CSIRT will begin its investigations and report the findings to standards written for how the CSIRT will be trained and what authority the members will be granted.

A good standard will define when the CSIRT will contain and clean up incidents and when the team will watch and gather information for litigation.

Having good recovery procedures are essential. It is very rare to find a CSIRT member that has mastered every operating system and application in

your environment. Having procedures to follow on how to correctly down and restore a system can help prevent time consuming efforts and alleviate some of the stress of the incident.

These written procedures will aide the CSIRT in formalizing how investigations are carried out, how evidence is handled, what organizations are notified at what times, how post mortem reporting is conducted, how malicious software is to be eradicated and how to perform a recovery of a information system.

### iii) Code of Conduct

The code of conduct policy for the CSIRT is a set of rules outlining how a team member will behave in a way that supports the goals of the incident response team and the mission statement of the company. The code of conduct will be used when no other policy or procedure applies. It should reflect the natural behavior of a professional incident handler. An example of a CSIRT code of conduct policy was written by the original manager of the CERT,<sup>1</sup> Rich Pethia.

### iv) Disclosure Policy

It is important to define the CSIRT disclosure policy. Without the policy, the team will have no guidance on who to disclose to, what to disclose and when to disclose the information. Traditionally, CSIRT staff treated all

---

<sup>1</sup> CERT Coordination Center. .  
Tim Proffitt  
- 10 -

information reported to them as confidential and information around security incidents were not distributed to other organizations. In some cases, law enforcement or other response teams were included when coordinating the response to the incident.

The policy should outline the information disclosure restrictions placed on the CSIRT staff. What will be reported to law enforcement? If the incident involved the disclosure of personally identifiable information, when do you disclose to the affected individuals? Personal information includes, but is not limited to, information regarding a person's home or other personal address, driver's license, marital status, financial information, credit card numbers, bank accounts, parental status, sex, race, religion, political affiliation, personal assets, home or other personal phone numbers, and so on. Did the incident involve the disclosure of electronically protected healthcare information as defined in HIPAA?<sup>2</sup> Did the incident involve social security numbers? If the CSIRT is to engage law enforcement, can the business afford to have equipment confiscated?

The disclosure policy will specify (sometimes legal) limitations that outlines how or when law enforcement is notified, customers are notified, external CSIRTs and upper management.

There are very clear state laws in the United States that outline when companies must notify individuals that their personal information has been disclosed by unauthorized events. At least 35 states, as of Q1 2007, have

---

<sup>2</sup> <http://hipaa.yale.edu/guidance/index.html>

Tim Proffitt  
- 11 -

enacted legislation requiring companies and government agencies to disclose security breaches involving personal information<sup>3</sup>.

Arizona	Ariz. Rev. Stat. § <a href="#">44-7501</a>
Arkansas	Ark. Code § <a href="#">4-110-101 et seq.</a>
California	Cal. Civ. Code § <a href="#">1798.82</a>
Colorado	Col. Rev. Stat. § <a href="#">6-1-716</a>
Connecticut	Conn. Gen Stat. <a href="#">36A-701(b)</a>
Delaware	De. Code <a href="#">tit. 6, § 12B-101 et seq.</a>
Florida	Fla. Stat. § <a href="#">817.5681</a>
Georgia	Ga. Code § <a href="#">10-1-910 et seq.</a>
Hawaii	Hawaii Rev. Stat. § <a href="#">487N-2</a>
Idaho	Id. Code §§ <a href="#">28-51-104 to 28-51-107</a>
Illinois	815 Ill. Comp. Stat. <a href="#">530/1 et seq.</a>
Indiana	Ind. Code § <a href="#">24-4.9</a>
Kansas	50-7a01, 50-7a02 <a href="#">2006 S.B. 196</a> ,
Louisiana	La. Rev. Stat. § <a href="#">51:3071 et seq.</a>
Maine	Me. Rev. Stat. tit. 10 §§ <a href="#">1347 et seq.</a>
Michigan	<a href="#">2006 S.B. 309, Public Act 566</a>
Minnesota	Minn. Stat. § <a href="#">325E.61</a> , § <a href="#">609.891</a>
Montana	Mont. Code § <a href="#">30-14-1701 et seq.</a>
Nebraska	Neb. Rev Stat <a href="#">87-801 et. seq.</a>
Nevada	Nev. Rev. Stat. <a href="#">603A.010 et seq.</a>
New Hampshire	N.H. RS <a href="#">359-C:19 et seq.</a>
New Jersey	N.J. Stat. <a href="#">56:8-163</a>
New York	N.Y. Bus. Law § <a href="#">899-aa</a>
North Carolina	N.C. Gen. Stat § <a href="#">75-65</a>
North Dakota	N.D. Cent. Code § <a href="#">51-30-01 et seq.</a>
Ohio	Ohio Rev. Code § <a href="#">1349.19</a> , § <a href="#">1347 et seq.</a>
Oklahoma	Okla. Stat. § <a href="#">74-3113.1</a>
Pennsylvania	73 Pa. Cons. Stat. §
Rhode Island	R.I. Gen. Laws § <a href="#">11-49.2-1 et seq.</a>
Tennessee	Tenn. Code § <a href="#">47-18-2107</a>

<sup>3</sup> <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>

Texas	Tex. Bus. & Com. Code § <a href="#">48.001 et seq.</a>
Utah	Utah Code § <a href="#">13-44-101 et seq.</a>
Vermont	Vt. Stat. Tit. 9 § <a href="#">2430 et seq.</a>
Washington	Wash. Rev. Code § <a href="#">19.255.010</a>
Wisconsin	Wis. Stat. § <a href="#">895.507</a>

Timing of a disclosure event is imperative. It is important to perform incident investigations and be as certain as possible about the disclosure events. At the same time the CSIRT should be notifying the victims as soon as possible. If the duration between the identification and the notification are too great, the company can face litigation and even greater loss of public opinion.<sup>4</sup> It is imperative that the CSIRT utilize legal council when drafting a disclosure communication to anyone as this notification can have enormous consequences to the company's reputation.

#### Disclosure Procedures to External CSIRT

There will be times where the company CSIRT will want to notify external CSIRT such as the CERT/CC, FIRST<sup>5</sup>, or private Managed Security Solutions Partners (MSSP). To be successful, it is important that coordination occurs among law enforcement, National CSIRTs and the research community who have experience in responding to security incidents. External CSIRTs can play an important role by helping their constituents protect their systems, detect, identify, and analyze compromises to the security of those systems and effectively coordinate the response to the attack. External CSIRT teams

---

<sup>4</sup> <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

<sup>5</sup> <http://www.first.org/members/teams/>

Tim Proffitt  
- 13 -

can also be evangelists in promoting and helping other organizations build effective incident management capabilities.

The details for sharing of information will change depending on the incident and how the external CSIRT will benefit from the information. Information is typically disclosed to:

- Inform other CSIRT of a large attack.
- Inform other teams about a new vulnerability or attack vector.
- Contact other sites that are the target of an incident to help coordinate the remediation.

Procedures should be clearly written for the internal CSIRT to follow when submitting an incident outside the organization. When reporting intruder activity, it is important to ensure that you provide enough information for the external CSIRT to be able to understand and respond to your report, but still filter any information that would be considered sensitive to the company.

#### v) Evidence Handling Procedures

During the CSIRT's active services, it is important to track information pertaining to the incident. This tracking of information should be at a level of detail that can be useful for recalling the event years later. Handling procedures should record information in logical organized methods to provide historical records and actions taken by the team. In many cases, this information can be used for statistical reporting purposes in management

Tim Proffitt  
- 14 -

reports. For every incident, best practices capture and track, at a minimum, the following set of information:

- Local Tracking Number / External CSIRT Tracking Number
- Category of Incident
  - o Disclosure, Hacking Attempt, Worm Outbreak, Malicious Insider, etc.
- Brief Description
- Contacts for all Parties Involved
- Subjective Priority
  - o Critical, High, Medium, Low, Informational
- Evidence Gathered
  - o who, what, where, why, how, when
- History of Actions
  - o Record all actions by the team. This will be important if litigation is an optional outcome.
- Current Status of the Incident
  - o Active, On Hold, Complete, etc.

CSIRT should utilize electronic collaboration tools such as a Microsoft SharePoint Server. Team members should have a single point to deposit, search, and update data on incident activities. Additionally, incidents should be archived for some predetermined period of time, using the collaboration tool. The SharePoint tool allows for a repository of electronic data, online workflow capabilities, versioning, automatic alerting and very flexible role



based access for team members and additional stake holders outside the team.

Physical evidence should be maintained in a designated “war room”. An empty office or conference room can be converted into a CSIRT war room with the understanding that the team will have sole access to a physically secured room. Locking cabinets for hard drives, tapes, and notes on tracking of the equipment are a must.

## 2) Primary Phases of the CSIRT

The functions that the CSIRT perform during active services are going to be considered the heart of the CSIRT mission. These primary functions are preparation, identification, containment, eradication, recovery, and lessons learned.

### a) Identification

How does the company detect an event? What triggers the CSIRT into action? The answer for most is a mixed one.

- Technology departments deploy intrusion prevention sensors, monitor firewall logs, review honeypot activity<sup>6</sup>, analyze antivirus alerts, review vulnerability assessment reports, examine authentication events, etc.

---

<sup>6</sup> <http://www.honeynet.org> is a popular open source honeypot project  
Tim Proffitt

- Business units will typically educate and raise awareness about security risks to make the workforce use their eyes and ears to identify suspicious activity.

When either of these groups detects an event, the CSIRT should be notified.

#### i) Triage Role

The goal of the triage role is to ensure that information about an event is gathered from a single point of contact. The triage role is the primary contact for the CSIRT for the business. Contacted by email, fax, telephone, anonymous form, or hallway conversation, the triage role will kick off the incident procedures by calling into action the correct team members to start the investigation.

The company should be trained on how to report information to the CSIRT. The triage role should be clearly defined, contact methods should be easily accessible, simple and defined procedures for reporting and clear guidelines on types of events to be reported.

#### ii) Identification Tasks

The CSIRT should have a member of the management team as its sponsor. This is typically the CSO, CIO or VP over the technology department. Notify your sponsor that an investigation has started. If

additional resources are needed outside the CSIRT, the sponsor will help with obtaining what is needed.

It is in the identification function that a primary incident handler should be assigned. The responsibility of the primary handler is to ensure coordination, documentation, and communication with the CSIRT and any other departments or organizations<sup>7</sup> directly involved. The primary handler will be responsible for the quality of the incident handling procedures for the assigned event.

The information gathered in this identification phase is critical. The first goal of the team is to determine whether the incident reported is actually an incident. The team will be asking assessment questions such as, what are the affected systems, if a vulnerability is present, the value of the system to the business (i.e. mission critical), can the vulnerability be exploited remotely, was this incident user error, was data exposed to unauthorized individuals, does this incident affect companies outside our own?

Be sure to establish good chain of custody scenarios. Document the “who, what, where, when”, whenever possible. Each piece of evidence must be under the control of a CSIRT member at all times and document the storage of evidence if it is secured. The chain of custody will be important for law enforcement if the evidence is going to be used in litigation.

---

<sup>7</sup> See appendix for law enforcement contact information  
Tim Proffitt

## b) Containment

The containment function is designed to prevent the attack from affecting systems, people, or organizations any more than it has already. The CSIRT is now trying to keep the scenario from getting worse.

A decision must be made when entering the containment phase. If evidence collected is going to be used for litigation, care must be taken to keep the system(s) from becoming contaminated by the containment efforts. Drives should be imaged, back ups performed, original copies secured, etc. Always use a backup or a copy to perform the incident handling procedures.

The CISRT should perform multiple backups as soon as it is practical. The backups can be used for forensics or in the off chance that containment procedures render the system(s) inoperable. In most cases, original media will be cataloged and secured, while a backup copy will be used to restore the system for eradication and recovery.

The containment phase can involve many tasks: Patching systems, password changes, firewall rule changes, account management, stopping of services and RootKit / Antivirus system scans. On the employee side the CSIRT may place phone calls to halt a business process, obtain paper materials or printouts that contain false information or send a corporate wide communication to alert the workforce.

### c) Eradication

The eradication phase involves the removal of any malicious activity or artifacts left by the intrusion. Typically eradication engages in removing virus infections, backdoor software, data left by the intruder and uninstalling attack tools. If the system was hit with any flavor of a rootkit, formatting hard drives, reloading the system, patching and restoration from backup is highly recommended.

Vulnerability assessment and analysis is typically performed during the eradication phase. Initiating system and network level vulnerability scans will help the team find open vulnerabilities. In many cases, attackers often use the same vulnerability across the entire network. A quality scanner such as Qualys<sup>8</sup> or Foundscan can go a long way in providing your CSIRT will vulnerability data. The CSIRT should research the vulnerability against the known information repositories such as CERT or BugTraq to understand the impact of the exploit against the company.

Improving the defenses of the systems or business process affected is vital. New firewall rules, host based intrusion prevention technologies, upgrades to more secure applications and patching are good techniques for improving the defenses. If the vulnerability is not removed, the system can become compromised all over. Business process can be strengthened by objectives such as implementing least access principles, encryption mechanisms and social engineering awareness.

---

<sup>8</sup> [http://www.qualys.com/solutions/vulnerability\\_management/](http://www.qualys.com/solutions/vulnerability_management/)

Tim Proffitt  
- 20 -

## d) Recovery

The recovery phase is used to bring the restored system(s) back into production. Recovery will typically take place, according to the system owner, after business unit testing has been conducted.

Monitoring is an important objective during this phase. When the incident system(s) are brought back into production use, monitoring must be conducted to validate the eradication was successful. Auditing the operating system logs, intrusion detection or prevention logs, checking for backdoor ports, reviewing firewall logs and searching for any new vulnerabilities are standard procedures.

## e) Lessons Learned

The best way to improve on a company's defense is to learn from the mistakes made. The goal of the lessons learned reporting is to finalize the CSIRT documentation, and create a post mortem report for review. In most cases, a meeting is scheduled within a week to review the report. The report should focus on events leading up to the incident, generally what occurred, what was done to contain and eradicate, and what can be done to mitigate the vulnerability in the future. The reporting phase is a good time to note organizational problems that conflicted with the CSIRT's procedures and suggest improvements. Invite the correct management, stake holders and information technology individuals to better expose the CSIRT's efforts. The

Tim Proffitt  
- 21 -

lessons learned meetings can be a good place to obtain approval to fix business processes, obtain newer technologies, update incident handling procedures and to educate the business.

It is important to have the CSIRT members involved in the incident complete the lessons learned documentation as close to completing the incident as possible. These post mortem reports should be short but professional and designed for executive consumption.

### 3) CSIRT Membership

Outsiders may view the CSIRT as a team of highly educated technologists. Although technical experience is a good prerequisite, there are several attributes that are needed for a successful incident team. It is important for the company's management team to understand the needs of the CSIRT. Specific incident response training, paid time off, and membership buy in from across the company are several topics that will need to be agreed upon.

#### a) CSIRT Staff

One of the challenging facets of building a successful incident response team is to employ a multifaceted team. A typical team will have the following schema:

- Primary Members

- Technology Security Specialists
- System Administrators
- Network Engineers
- Desktop Support Specialists
- Disaster Recovery Coordinators
- Secondary Members
  - Inside Legal Council
  - Corporate HR Specialist
  - Corporate Communication Specialist
  - Physical Security or Facilities Coordinator
  - Management Team Sponsor

Geographically diverse companies will need to work out the combination of remote handlers with a centralized team. The primary members will be the core of the CSIRT and will work the majority of the smaller incidents. The secondary members will be expected to join the CSIRT when an event requires their expertise. A hoax email virus infection will not require the secondary members to be called into action, but payroll laptops going missing will no doubt call the entire team into action.

### Interpersonal Skills

Having a wide range of skills is a high priority, but communication skills will greatly improve the reputation of the team. You may find expert security engineers that would seem to be a fit in the CSIRT except for a lack of interpersonal skills. The team members should have common sense, exhibit



effective oral and written communication skills, show diplomacy when dealing with external groups, have the ability to follow standards and procedures, show integrity and have the willingness to continue their education.

## Technical Skills

Technical skills will be important for a successful CSIRT. The primary members of the team will need to have a good amount of experience in their individual fields to effectively handle a security incident. Senior network engineers, senior system administrators, and senior security specialists will be good candidates for membership. The technical understanding provided by the experienced primary members will be needed for the large variety of incident scenarios that will be investigated.

### b) CSIRT Training

Training of the CSIRT is important. Training will increase the skills of the team as new technologies are available, keep the team practiced, and educate the newest members.

Training should focus not only on forensic analysis and eradication techniques, but other general skills in communication, project management, evidence handling, team building, intruder techniques, compliancy laws, privacy laws and ethics. The team should be periodically evaluated to determine ways to expand the skills that would increase the competency of the CSIRT.

Technical skills such as, but not limited to, firewall technologies, router and switch infrastructures, TCP/IP, Operating system installation and hardening, security event manager concepts, intrusion prevention technologies, vulnerability assessment techniques, wireless infrastructures, secure programming concepts, etc. should always be kept current.

New team members can be overwhelmed with the standards and procedures that they will be introduced to as an incident handler. In most cases, new CSIRT members will be paired with an experienced handler as a mentor. As the new team member becomes familiar with the roles of an incident handler, they can be used to draft communications, compose lessons learned reports for review, aide in research or work with evidence documentation.

### c) Extensions of the CSIRT

A CSIRT, on occasion, may find that it will be unable to staff full time members. In these cases the CSIRT will need to develop good relationships with the subject matter experts needed when an incident is being investigated. The CSIRT policy can outline how outside employees can be called into service of the incident team when a set of criteria is met. You will see this situation more often for the human resources, legal council and physical facilities members. The management team should be clear on when the CSIRT can utilize these head count and what priority can be used. This standard

should be well established in advance so that these extended staff can be called into action quickly.

## 4) Conclusion

Using good communication skills, clear policies, professional team members and utilizing training opportunities, a company can run a successful incident response team. CSIRTs will continue to serve as an important component in supporting the management of risk and security in the business. By utilizing these passive and active phases of a CSIRT, the business will improve its security efforts across the enterprise and protect confidentiality, integrity and availability of its information systems.

## 5) References

CERT. Handbook for Computer Security Incident Response Teams (CSIRTs)

CERT. Defining Incident Management Processes for CSIRTs: A Work in Progress

SANS. Incident Handling Step-by-Step and Computer Crime Investigation: Book 1

CERT. "CSIRT Code of Conduct." Materials from the course *Managing Computer Security Incidence Response Teams(CSIRTS)*.

National Conference of State Legislatures.

<http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>

Microsoft. "Fundamental Computer Investigation Guide for Windows"

<http://www.microsoft.com/technet/SolutionAccelerators>

Federal Bureau of Investigation

<http://www.fbi.gov/contact/fo/fo.htm>

© SANS Institute 2007, Author retains full rights.

## Appendix A

### FBI & Secret Service FIELD OFFICES

<p><b>ALABAMA</b></p> <p><b>Birmingham</b> FBI 205.326.6166/205.715.0232 2121 8th Avenue N. Birmingham, AL 35203-2396 USSS 205.731.1144/205.731.0007 Daniel Building 15 South 20th Street, Suite 1125 Birmingham, AL 35233</p> <p><b>Mobile</b> FBI 334.438.3674/251.415.3235 One St. Louis Centre 1 St. Louis Street, 3rd Floor Mobile, AL 36602-3930 USSS 334.441.5851/334.441.5250 Parkview Office Building 182 St. Francis Street Mobile, AL 36602</p> <p><b>Montgomery</b> USSS 334.223.7601/334.223.7523 Colonial Financial Center 1 Commerce Street, Suite 605 Montgomery, AL 36104</p> <p><b>ALASKA</b></p> <p><b>Anchorage</b> FBI 907.276.4441/907.265.9599 101 East Sixth Avenue Anchorage, AK 99501-2524 USSS 907.271.5148/907.271.3727 Federal Building &amp; U.S. Courthouse 222 West 7th Avenue, Room 559 Anchorage, AK 99513</p> <p><b>ARIZONA</b></p> <p><b>Phoenix</b> FBI 602.279.5511/602.650.3024 201 East Indianola Avenue, Suite 400 Phoenix, AZ 85012-2080 USSS 602.640.5580/602.640.5505 3200 North Central Avenue, Suite 1450 Phoenix, AZ 85012</p> <p><b>Tucson</b> USSS 520.670.4730/520.670.4826 300 West Congress Street, Room 4-V Tucson, AZ 85701</p> <p><b>ARKANSAS</b></p> <p><b>Little Rock</b> FBI 501.221.9100/501.228.8509 24 Shackelford West Boulevard Little Rock, AR 72211-3755 USSS 501.324.6241/501.324.6097 111 Center Street, Suite 1700 Little Rock, AR 72201-4419</p>	<p><b>CALIFORNIA</b></p> <p><b>Fresno</b> USSS 209.487.5204/559.487.5013 5200 North Palm Avenue, Suite 207 Fresno, CA 93704</p> <p><b>Los Angeles</b> FBI 310.477.6565/310.996.3359 Federal Office Building  11000 Wilshire Boulevard, Suite 1700 Los Angeles, CA 90024-3672 USSS 213.894.4830 213.894.2948 Roybal Federal Building 255 East Temple Street, 17th Floor Los Angeles, CA 90012</p> <p><b>Riverside</b> USSS 909.276.6781/909.276.6637 4371 Latham Street, Suite 203 Riverside, CA 92501</p> <p><b>Sacramento</b> FBI 916.481.9110/916.977.2300 4500 Orange Grove Avenue Sacramento, CA 95841-4205 USSS 916.930.2130/916.930.2140 501 I Street, Suite 9500 Sacramento, CA 95814-2322</p> <p><b>San Diego</b> FBI 858.565.1255/858.499.7991 Federal Office Building 9797 Aero Drive San Diego, CA 92123-1800 USSS 619.557.5640/619.557.6658 550 West C Street, Suite 660 San Diego, CA 92101</p> <p><b>San Francisco</b> FBI 415.553.7400/415.553.7674 450 Golden Gate Avenue, 13th Floor San Francisco, CA 94102-9523 USSS 415.744.9026/415.744.9051 345 Spear Street San Francisco, CA 94105</p> <p><b>San Jose</b> USSS 408.535.5288/408.535.5292 U.S. Courthouse &amp; Federal Building 280 S. First Street, Suite 2050 San Jose, CA 95113</p> <p><b>Santa Ana</b> USSS 714.246.8257/714.246.8261 200 W. Santa Ana Boulevard, Suite 500 Santa Ana, CA 92701-4164</p> <p><b>Ventura</b> USSS 805.339.9180/805.339.0015 5500 Telegraph Road, Suite 161 Ventura, CA 93003</p>	<p><b>COLORADO</b></p> <p><b>Colorado Springs</b> USSS 719.632.3325/719.632.3341 212 N. Wahsatch, Room 204 Colorado Springs, CO 80903</p> <p><b>Denver</b> FBI 303.629.7171/303.628.3085 1961 Stout Street, 18th Floor Denver, CO 80294-1823 USSS 303.866.1010/303.866.1934 1660 Lincoln Street Denver, CO 80264</p> <p><b>CONNECTICUT</b></p> <p><b>New Haven</b> FBI 203.777.6311/203.503.5098 600 State Street New Haven, CT 06511-6505 USSS 203.865.2449/203.865.2525 265 Church Street, Suite 1201 New Haven, CT 06510</p> <p><b>DELAWARE</b></p> <p><b>Wilmington</b> USSS 302.573.6188/302.573.6190 One Rodney Square 920 King Street, Suite 414 Wilmington, DE 19801</p> <p><b>DISTRICT OF COLUMBIA</b></p> <p><b>Washington, D.C.</b> FBI (HDQRS.) 202.278.2000/202.278.2478 601 4th Street NW Washington, D.C. 20535-0002  USSS 202.406.8000/202.406.8803 1100 L Street NW, Suite 6000 Washington, D.C. 20005 USSS (HDQRS.) 202.406.5850/202.406.5031 950 H Street NW Washington, D.C. 20223</p>
---	--	--

Tim Proffitt  
- 28 -

Creating and Managing an Incident  
Response Team for a Large Company

<p><b>FLORIDA</b></p> <p><b>Jacksonville</b> FBI 904.721.1211/904.727.6242 7820 Arlington Expressway Jacksonville, FL 32211-7499 USSS 904.296.0133/904.296.0188 7820 Arlington Expressway, Suite 500 Jacksonville, FL 32211</p> <p><b>Miami</b> FBI 305.944.9101/305.787.6538 16320 NW Second Avenue North Miami Beach, FL 33169-6508 USSS 305.629.1800/305.629.1830 8375 NW 53rd Street Miami, FL 33166</p> <p><b>Orlando</b> USSS 407.648.6333/407.648.6606 135 West Central Boulevard, Suite 670 Orlando, FL 32801</p> <p><b>Tallahassee</b> USSS 850.942.9523/850.942.9526 Building F 325 John Knox Road Tallahassee, FL 32303</p> <p><b>Tampa</b> FBI 813.273.4566/813.272.8019 Federal Office Building 500 Zack Street, Room 610 Tampa, FL 33602-3917 USSS 813.228.2636/813.228.2618 501 East Polk Street, Room 1101 Tampa, FL 33602</p> <p><b>West Palm Beach</b> USSS 561.659.0184/561.655.8484 505 South Flagler Drive West Palm Beach, FL 33401</p> <p><b>GEORGIA</b></p> <p><b>Albany</b> USSS 229.430.8442/229.430.8441 Albany Tower 235 Roosevelt Avenue, Suite 221 Albany, GA 31702</p> <p><b>Atlanta</b> FBI 404.679.9000/404.679.6289 2635 Century Parkway Northeast, Suite 400 Atlanta, GA 30345-3112 USSS 404.331.6111/404.331.5058 401 West Peachtree Street, Suite 2906 Atlanta, GA 31702</p> <p><b>Savannah</b> USSS 912.652.4401/912.652.4062 33 Bull Street Savannah, GA 31401</p>	<p><b>HAWAII</b></p> <p><b>Honolulu</b> FBI 808.566.4300/808.566.4470 Kalaniana'ole Federal Office Building 300 Ala Moana Boulevard, Room 4-230 Honolulu, HI 96850-0053</p> <p>USSS 808.541.1912/808.545.4490 Kalaniana'ole Federal Office Building 300 Ala Moana Boulevard, Room 6-210 Honolulu, HI 96850</p> <p><b>IDAHO</b></p> <p><b>Boise</b> USSS 208.334.1403/208.334.1289 Federal Building - U.S. Courthouse 550 West Fort Street, Room 730 Boise, ID 83724-0001</p> <p><b>ILLINOIS</b></p> <p><b>Chicago</b> FBI 312.421.4310/312.786.2525 E.M. Dirksen Federal Office Building 219 South Dearborn Street, Room 905 Chicago, IL 60604-1702</p> <p>USSS 312.353.5431/312.353.1225 Gateway IV Building 300 S. Riverside Plaza, Suite 1200 North Chicago, IL 60606</p> <p><b>Springfield</b> FBI 217.522.9675/217.535.4440 400 West Monroe Street, Suite 400 Springfield, IL 62704-1800 USSS 217.492.4033/217.492.4680 400 West Monroe Street, Suite 301 Springfield, IL 62704</p> <p><b>INDIANA</b></p> <p><b>Evansville</b> USSS 812.985.9502/812.985.9504 P.O. Box 530 Newburgh, IN 47630</p> <p><b>Indianapolis</b> FBI 317.639.3301/317.321.6193 Federal Office Building 575 N. Pennsylvania Street, Room 679 Indianapolis, IN 46204-1585</p> <p>USSS 317.226.6444/317.226.5494 Federal Office Building 575 N. Pennsylvania Street, Suite 211 Indianapolis, IN 46204-1585</p> <p><b>South Bend</b> USSS 219.273.3140/219.271.9301 P.O. Box 477 South Bend, IN 46625</p>	<p><b>IOWA</b></p> <p><b>Des Moines</b> USSS 515.284.4565/515.284.4566 210 Walnut Street, Suite 637 Des Moines, IA 50309-2107</p> <p><b>KANSAS</b></p> <p><b>Wichita</b> USSS 316.269.6694/316.269.6154 Epic Center 301 N. Main Street, Suite 275 Wichita, KS 67202</p> <p><b>KENTUCKY</b></p> <p><b>Lexington</b> USSS 859.223.2358/859.223.1819 3141 Beaumont Centre Circle Lexington, KY 40513</p> <p><b>Louisville</b> FBI 502.583.3941/502.569.3869 Federal Building 600 Martin Luther King Jr. Place, Room 500 Louisville, KY 40202-2231 USSS 502.582.5171/502.582.6329 Federal Building 600 Martin Luther King Jr. Place, Room 377 Louisville, KY 40202-2231</p> <p><b>LOUISIANA</b></p> <p><b>Baton Rouge</b> USSS 225.389.0763/225.389.0325 One American Place, Suite 1502 Baton Rouge, LA 70825</p> <p><b>New Orleans</b> FBI 504.816.3000/504.816.3306 2901 Leon C. Simon Drive New Orleans, LA 70126 USSS 504.589.4041/504.589.6013 Hale Boggs Federal Building 501 Magazine Street New Orleans, LA 70130</p> <p><b>Shreveport</b> USSS 318.676.3500/318.676.3502 401 Edwards Street Shreveport, LA 71101</p> <p><b>MAINE</b></p> <p><b>Portland</b> USSS 207.780.3493/207.780.3301 100 Middle Street West Tower, 2nd Floor Portland, ME 04101</p>
---	--	--

Tim Proffitt  
- 29 -

@ SANS 2007

As Part of the Information Security Reading Room  
Author retains full rights

© SANS Institute 2007,

As part of the Information Security Reading Room

Author retains full rights.

Creating and Managing an Incident  
Response Team for a Large Company

<p><b>MARYLAND</b></p> <p><b>Baltimore</b> FBI 410.265.8080/410.281.0339 7142 Ambassador Road Baltimore, MD 21244-2754 USSS 410.962.2200/410.962.0840 100 S. Charles Street, 11th Floor Baltimore, MD 21201</p> <p><b>Eastern Shore</b> USSS 410.268.7286/410.268.7903 U.S. Naval Academy Police Dept., Headquarters Building 257, Room 221 Annapolis, MD 21402</p> <p><b>Frederick</b> USSS 301.293.6434/301.694.8078 Rowley Training Center 9200 Powder Mill Road, Route 2 Laurel, MD 20708</p>	<p><b>MISSISSIPPI</b></p> <p><b>Jackson</b> FBI 601.948.5000/601.360.7550 Federal Building 100 West Capitol Street Jackson, MS 39269-1601 USSS 601.965.4436/601.965.4012 Federal Building 100 West Capitol Street, Suite 840 Jackson, MS 39269</p> <p><b>MISSOURI</b></p> <p><b>Kansas City</b> FBI 816.512.8200/816.512.8545 1300 Summit Kansas City, MO 64105-1362 USSS 816.460.0600/816.283.0321 1150 Grand Avenue, Suite 510 Kansas City, MO 64106</p> <p><b>Springfield</b> USSS 417.864.8340/417.864.8676 901 St. Louis Street, Suite 306 Springfield, MO 65806</p> <p><b>St. Louis</b> FBI 314.231.4324/314.589.2636 222 Market Street St. Louis, MO 63103-2516 USSS 314.539.2238/314.539.2567 Thomas F. Eagleton U.S. Courthouse 111 S. 10th Street, Suite 11.346 St. Louis, MO 63102</p>	<p><b>NEW HAMPSHIRE</b></p> <p><b>Manchester</b> USSS 603.626.5631/603.626.5653 1750 Elm Street, Suite 802 Manchester, NH 03104</p> <p><b>NEW JERSEY</b></p> <p><b>Atlantic City</b> USSS 609.487.1300/609.487.1491 Ventnor Professional Campus 6601 Ventnor Avenue Ventnor City, NJ 08406</p> <p><b>Newark</b> FBI 973.792.3000/973.792.3035 1 Gateway Center, 22nd Floor Newark, NJ 07102-9889 USSS 973.656.4500/973.984.5822 Headquarters Plaza, West Towers, Speedwell Avenue, Suite 700 Morristown, NJ 07960</p> <p><b>Trenton</b> USSS 609.989.2008/609.989.2174 402 East State Street, Suite 3000 Trenton, NJ 08608</p>
<p><b>MASSACHUSETTS</b></p> <p><b>Boston</b> FBI 617.742.5533/617.223.6327 One Center Plaza, Suite 600 Boston, MA 02108 USSS 617.565.5640/617.565.5659 Thomas P. O'Neill Jr. Federal Building 10 Causeway Street Boston, MA 02222</p> <p><b>MICHIGAN</b></p> <p><b>Detroit</b> FBI 313.965.2323/313.237.4009 Patrick V. McNamara Building 477 Michigan Avenue, 26th Floor Detroit, MI 48226 USSS 313.226.6400/313.226.3952 Patrick V. McNamara Building 477 Michigan Avenue Detroit, MI 48226</p> <p><b>Grand Rapids</b> USSS 616.454.4671/616.454.5816 330 Ionia Avenue NW, Suite 302 Grand Rapids, MI 49503-2350</p> <p><b>Saginaw</b> USSS 989.752.8076/989.752.8048 301 E. Genesee, Suite 200 Saginaw, MI 48607</p>	<p><b>MONTANA</b></p> <p><b>Great Falls</b> USSS 406.452.8515/406.761.2316 11 Third Street North Great Falls, MT 59401</p> <p><b>NEBRASKA</b></p> <p><b>Omaha</b> FBI 402.493.8688/402.492.3799 10755 Burt Street Omaha, NE 68114-2000 USSS 402.965.9670/402.445.9638 2707 North 108 Street, Suite 301 Omaha, NE 68164</p>	<p><b>NEW MEXICO</b></p> <p><b>Albuquerque</b> FBI 505.224.2000/505.224.2276 415 Silver Avenue SW, Suite 300 Albuquerque, NM 87102 USSS 505.248.5290/505.248.5296 505 Marquette Street NW Albuquerque, NM 87102</p>
<p><b>MINNESOTA</b></p> <p><b>Minneapolis</b> FBI 612.376.3200/612.376.3249 111 Washington Avenue South, Suite 1100 Minneapolis, MN 55401-2176 USSS 612.348.1800/612.348.1807 U.S. Courthouse 300 South 4th Street, Suite 750 Minneapolis, MN 55415</p>	<p><b>NEVADA</b></p> <p><b>Las Vegas</b> FBI 702.385.1281/702.385.1281 John Lawrence Bailey Building 700 East Charleston Boulevard Las Vegas, NV 89104-1545 USSS 702.388.6571/702.388.6668 600 Las Vegas Boulevard South, Suite 600 Las Vegas, NV 89101</p> <p><b>Reno</b> USSS 775.784.5354/775.784.5991 100 West Liberty Street, Suite 850 Reno, NV 89501</p>	

Tim Proffitt  
- 30 -

Creating and Managing an Incident  
Response Team for a Large Company

NEW YORK	NORTH CAROLINA	OKLAHOMA
<p><b>Albany</b> FBI 518.465.7551/518.431.7463 200 McCarty Avenue Albany, NY 12209 USSS 518.436.9600/518.436.9635 39 North Pearl Street, 2nd Floor Albany, NY 12207</p>	<p><b>Charlotte</b> FBI 704.377.9200/704.331.4595 Wachovia Building 400 South Tyron Street, Suite 900 Charlotte, NC 28285-0001 USSS 704.442.8370/704.442.8369 One Fairview Center 6302 Fairview Road Charlotte, NC 28210</p>	<p><b>Oklahoma City</b> FBI 405.290.7770/405.290.3885 3301 West Memorial Drive Oklahoma City, OK 73134 USSS 405.810.3000/405.810.3098 Lakepoint Towers 4013 NW Expressway, Suite 650 Oklahoma City, OK 73116</p>
<p><b>Buffalo</b> FBI 716.856.780/716.843.5288 One FBI Plaza Buffalo, NY 14202-2698 USSS 716.551.4401/716.551.5075 610 Main Street, Suite 300 Buffalo, NY 14202</p>	<p><b>Greensboro</b> USSS 336.547.4180/336.547.4185 4905 Koger Boulevard, Suite 220 Greensboro, NC 27407</p>	<p><b>Tulsa</b> USSS 918.581.7272 Pratt Tower 125 West 15th Street, Suite 400 Tulsa, OK 74119</p>
<p><b>JFK</b> USSS 718.553.0911/718.553.7626 John F. Kennedy Int'l. Airport Building 75, Room 246 Jamaica, NY 11430</p>	<p><b>Raleigh</b> USSS 919.790.2834/919.790.2832 4407 Bland Road, Suite 210 Raleigh, NC 27609</p>	<p><b>OREGON</b></p> <p><b>Portland</b> FBI 503.224.4181/503.552.5400 Crown Plaza Building 1500 SW 1st Avenue, Suite 400 Portland, OR 97201-5828 USSS 503.326.2162/503.326.3258 1001 SW 5th Avenue, Suite 1020 Portland, OR 97204</p>
<p><b>Melville</b> USSS 631.249.0404/631.249.0991 35 Pinelawn Road Melville, NY 11747</p>	<p><b>Wilmington</b> USSS 910.815.4511/910.815.4521 One Rodney Square 920 King Street, Suite 414 Wilmington, DE 19801</p>	
<p><b>New York</b> FBI 212.384.1000/212.384.2745 or 2746 26 Federal Plaza, 23rd Floor New York, NY 10278-0004 USSS 212.637.4500/212.637.4687 335 Adams Street, 32nd Floor Brooklyn, NY 11201</p>	<p><b>NORTH DAKOTA</b></p>	<p><b>PENNSLYVANIA</b></p>
<p><b>Rochester</b> USSS 716.263.6830/716.454.2753 Federal Building 100 State Street, Room 606 Rochester, NY 14614</p>	<p><b>Fargo</b> USSS 701.239.5070/701.239.5071 657 2nd Avenue North, Suite 302A Fargo, ND 58102 <b>OHIO</b></p>	<p><b>Philadelphia</b> FBI 215.418.4000/215.418.4232 William J. Green Jr. Federal Office Building 600 Arch Street, 8th Floor Philadelphia, PA 19106 USSS 215.861.3300/215.861.3311 7236 Federal Building 600 Arch Street Philadelphia, PA 19106</p>
<p><b>Syracuse</b> USSS 315.448.0304/315.448.0302 James Hanley Federal Building 100 S. Clinton Street, Room 1371 Syracuse, NY 13261</p>	<p><b>Cincinnati</b> FBI 513.421.4310/513.562.5650 John Weld Peck Federal Building 550 Main Street, Room 9000 Cincinnati, OH 45202-8501 USSS 513.684.3585/513.684.3436 John Weld Peck Federal Building 550 Main Street Cincinnati, OH 45202</p>	<p><b>Pittsburgh</b> FBI 412.471.2000/412.432.4188 U.S. Post Office Building 700 Grant Street, Suite 300 Pittsburgh, PA 15219-1906 USSS 412.395.6484/412.395.6349 1000 Liberty Avenue Pittsburgh, PA 15222</p>
<p><b>White Plains</b> USSS 914.682.6300/914.682.6182 140 Grand Street, Suite 300 White Plains, NY 10601</p>	<p><b>Cleveland</b> FBI 216.522.1400/216.622.6717 Federal Office Building 1240 East 9th Street, Room 3005 Cleveland, OH 44199-9912 USSS 216.706.4365/216.706.4445 6100 Rockside Woods Boulevard Suite 440 Cleveland, OH 44131-2334</p>	<p><b>Scranton</b> USSS 570.346.5781/570.346.3003 235 N. Washington Avenue, Suite 247 Scranton, PA 18501</p>
	<p><b>Columbus</b> USSS 614.469.7370/614.469.2049 500 South Front Street, Suite 800 Columbus, OH 43215</p>	
	<p><b>Dayton</b> USSS 937.225.2900/937.225.2724 Federal Building 200 West Second Street, Room 811 Dayton, OH 45402</p>	
	<p><b>Toledo</b> USSS 419.259.6434/419.259.6437 4 Seagate Center, Suite 702 Toledo, OH 43604</p>	

Tim Proffitt  
- 31 -



Creating and Managing an Incident  
Response Team for a Large Company

<p><b>RHODE ISLAND</b></p> <p><b>Providence</b> USSS 401.331.6456/401.528.4394 The Federal Center 380 Westminster Street, Suite 343 Providence, RI 02903</p> <p><b>SOUTH CAROLINA</b></p> <p><b>Charleston</b> USSS 843.747.7242/843.747.7787 5900 Core Avenue, Suite 500 North Charleston, SC 29406</p> <p><b>Columbia</b> FBI 803.551.4200/803.551.4324 151 Westpark Boulevard Columbia, SC 29210-3857 USSS 803.765.5446/803.765.5445 1835 Assembly Street, Suite 1425 Columbia, SC 29201</p> <p><b>Greenville</b> USSS 864.233.1490/864.235.6237 NCNB Plaza 7 Laurens Street, Suite 508 Greenville, SC 29601</p> <p><b>SOUTH DAKOTA</b></p> <p><b>Sioux Falls</b> USSS 605.330.4565/605.330.4523 230 South Phillips Avenue, Suite 405 Sioux Falls, SD 57104</p> <p><b>TENNESSEE</b></p> <p><b>Chattanooga</b> USSS 423.752.5125/423.752.5130 Post Office Building 900 Georgia Avenue, Room 204 Chattanooga, TN 37402</p> <p><b>Knoxville</b> FBI 865.544.0751/865.544.3590 John J. Duncan Federal Office Building 710 Locust Street, Suite 600 Knoxville, TN 37902-2537 USSS 865.545.4627/865.545.4633 John J. Duncan Federal Office Building 710 Locust Street, Room 517 Knoxville, TN 37902</p> <p><b>Memphis</b> FBI 901.747.4300/901.747.9621 Eagle Crest Building 225 North Humphreys Boulevard, Suite 3000 Memphis, TN 38120-2107 USSS 901.544.0333/901.544.0342 5350 Poplar Avenue, Suite 204 Memphis, TN 38119</p> <p><b>Nashville</b> USSS 615.736.5841/615.736.5848 658 U.S. Courthouse 801 Broadway Street Nashville, TN 37203</p>	<p><b>TEXAS</b></p> <p><b>Austin</b> USSS 512.916.5103/512.916.5365 Federal Office Building 300 E. 8th Street Austin, TX 78701</p> <p><b>Dallas</b> FBI 214.720.2200/214.922.7459 1801 North Lamar, Suite 300 Dallas, TX 75202-1795 USSS 972.868.3200/972.868.3232 125 East John W. Carpenter Freeway, Suite 300 Irving, TX 75062</p> <p><b>El Paso</b> FBI 915.832.5000/915.832.5259 660 S. Mesa Hills Drive El Paso, TX 79912 USSS 915.533.6950/915.533.8646 Mesa One Building 4849 North Mesa, Suite 210 El Paso, TX 79912</p> <p><b>Houston</b> FBI 713.693.5000/713.693.3999 2500 East TC Jester Houston, TX 77008-1300 USSS 713.868.2299/713.868.5093 602 Sawyer Street, Suite 500 Houston, TX 77007</p> <p><b>Lubbock</b> USSS 806.472.7347/806.472.7542 1205 Texas Avenue, Room 813 Lubbock, TX 79401</p> <p><b>McAllen</b> USSS 956.630.5811/956.630.5838 200 S. 10th Street, Suite 1107 McAllen, TX 78501</p> <p><b>San Antonio</b> FBI 210.225.6741/210.978.5380 U.S. Post Office Building 615 East Houston Street, Suite 200 San Antonio, TX 78205-9998 USSS 210.472.6175/210.472.6185 727 East Durango Boulevard, Suite B410 San Antonio, TX 78206-1265</p> <p><b>Tyler</b> USSS 903.534.2933 903.581.9569 6101 South Broadway, Suite 395 Tyler, TX 75703</p> <p><b>UTAH</b></p> <p><b>Salt Lake City</b> FBI 801.579.1400/801.579.4500 257 Towers Building 257 East 200 South, Suite 1200 Salt Lake City, UT 84111-2048 USSS 801.524.5910/801.524.6216 57 West 200 South Street, Suite 450 Salt Lake City, UT 84101</p> <p><b>VERMONT</b></p> <p>FBI 518.465.7551/518.431.7463 Contact field office located in Albany, NY USSS 617.565.5640/617.565.5659 Contact field office located in Boston, MA</p>	<p><b>VIRGINIA</b></p> <p><b>Norfolk</b> FBI 757.455.0100/757.455.2647 150 Corporate Boulevard Norfolk, VA 23502-4999 USSS 757.441.3200/757.441.3811 Federal Building 200 Granby Street, Suite 640 Norfolk, VA 23510</p> <p><b>Richmond</b> FBI 804.261.1044/804.627.4494 1970 East Parham Road Richmond, VA 23228 USSS 804.771.2274/804.771.2076 600 East Main Street, Suite 1910 Richmond, VA 23219</p> <p><b>Roanoke</b> USSS 540.345.4301/540.857.2151 105 Franklin Road SW, Suite 2 Roanoke, VA 24011</p> <p><b>WASHINGTON</b></p> <p><b>Seattle</b> FBI 206.622.0460/206.262.2587 1110 Third Avenue Seattle, WA 98101 USSS 206.220.6800/206.220.6479 890 Federal Building 915 Second Avenue Seattle, WA 98174</p> <p><b>Spokane</b> USSS 509.353.2532/509.353.2871 601 W. Riverside Avenue, Suite 1340 Spokane, WA 99201</p> <p><b>WEST VIRGINIA</b></p> <p><b>Charleston</b> USSS 304.347.5188/304.347.5187 5900 Core Avenue, Suite 500 North Charleston, SC 29406</p> <p><b>WISCONSIN</b></p> <p><b>Madison</b> USSS 608.264.5191/608.264.5592 131 W. Wilson Street, Suite 303 Madison, WI 53703</p> <p><b>Milwaukee</b> FBI 414.276.4684/414.276.6560 330 East Kilbourn Avenue Milwaukee, WI 53202 USSS 414.297.3587/414.297.3595 572 Courthouse 517 E. Wisconsin Avenue Milwaukee, WI 53202</p> <p><b>WYOMING</b></p> <p><b>Cheyenne</b> USSS 307.772.2380/307.772.2387 2120 Capitol Avenue, Suite 3026 Cheyenne, WY 82001</p>
--	---	--

Tim Proffitt  
- 32 -

@ SANS 2007

As Part of the Information Security Reading Room  
Author retains full rights

© SANS Institute 2007,

As part of the Information Security Reading Room

Author retains full rights.

© SANS Institute 2007, Author retains full rights.



# Upcoming SANS Training

[Click here to view a list of all SANS Courses](#)

SANS November Singapore 2018	Singapore, SG	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS Paris November 2018	Paris, FR	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS Austin 2018	Austin, TXUS	Nov 26, 2018 - Dec 01, 2018	Live Event
European Security Awareness Summit 2018	London, GB	Nov 26, 2018 - Nov 29, 2018	Live Event
SANS San Francisco Fall 2018	San Francisco, CAUS	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Stockholm 2018	Stockholm, SE	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Khobar 2018	Khobar, SA	Dec 01, 2018 - Dec 06, 2018	Live Event
SANS Nashville 2018	Nashville, TNUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Santa Monica 2018	Santa Monica, CAUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Dublin 2018	Dublin, IE	Dec 03, 2018 - Dec 08, 2018	Live Event
Tactical Detection & Data Analytics Summit & Training 2018	Scottsdale, AZUS	Dec 04, 2018 - Dec 11, 2018	Live Event
SANS Frankfurt 2018	Frankfurt, DE	Dec 10, 2018 - Dec 15, 2018	Live Event
SANS Cyber Defense Initiative 2018	Washington, DCUS	Dec 11, 2018 - Dec 18, 2018	Live Event
SANS Bangalore January 2019	Bangalore, IN	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS Sonoma 2019	Santa Rosa, CAUS	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Amsterdam January 2019	Amsterdam, NL	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Threat Hunting London 2019	London, GB	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Miami 2019	Miami, FLUS	Jan 21, 2019 - Jan 26, 2019	Live Event
Cyber Threat Intelligence Summit & Training 2019	Arlington, VAUS	Jan 21, 2019 - Jan 28, 2019	Live Event
SANS Dubai January 2019	Dubai, AE	Jan 26, 2019 - Jan 31, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NVUS	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LAUS	Feb 02, 2019 - Feb 09, 2019	Live Event
SANS Anaheim 2019	Anaheim, CAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Vienna, VAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, GB	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS ICS410 Perth 2018	OnlineAU	Nov 19, 2018 - Nov 23, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced