ON TARGET NEWSLETTER

A newsletter covering industrial security issues.

Volume 2, Issue 2 May 2008

In this issue:

ON TARGET NEWSLETTER
A security newsletter for MSU
Not approved for public release
Submit comments and questions to:
Neil E. Lewis, 5-8682

Reporting Responsibilities

One of your reporting responsibilities is to notify the Facility Security Office(r) of any changes in your status which could affect your security clearance. One of these changes is the removal of your security clearance. This can be done for a number of reasons; the completion of the contract that required you being cleared, terminating your employment with Mississippi State University for whatever reason or you no longer wish to have clearance. However it must be clearly understood that until you have notified the Facility Security Office (FSO) and have received and signed a debriefing statement, your security clearance is still valid and you must abide by all the rules and regulations. Just by you stating that I do not want a clearance anymore or the completion of the contract does not absolve you of your security responsibilities. The FSO must provide you a debriefing so that you know your continuing responsibilities to safeguard the information to which you had access.

Your debriefing and signing of the debriefing letter is of vital importance and one that I take very seriously. The process is painless, please if you no longer require your clearance for whatever reason, contact the FSO via telephone, 662-325-8682, or email, nelewis@fso.msstate.edu for the debriefing.

****

SCI, SCIF – What is it?

What do the terms SCI and SCIF mean and how do they affect security?

SCI stands for Sensitive Compartmented Information. This is a special category of national intelligence information concerning or derived from intelligence sources, methods or analytical processes, which is required to be handled within formal access control systems. To obtain access to SCI one must have the SCI access approval in conjunction with their collateral clearance. Think of a collateral clearance as a basic clearance either Secret or Top Secret with no additional access approvals. If you receive an SCI access approval with a TS collateral clearance, it is referred or written as TS/SCI. Consequently if you receive other access approvals they will be added to the

base clearance and you can end up with a clearance that looks like alphabet soup.

When you have been granted an SCI access approval you will receive another security briefing strictly relating to SCI. You will also be required to sign another Nondisclosure Agreement regarding your SCI access. This Nondisclosure Agreement will be stricter and more detailed then the one signed for your collateral clearance. The rules and regulations that personnel with SCI access must follow are stricter too. This is because you have access to more information that is of greater value to our adversaries, you have become a more inviting target.

Where does SCI information originate? Intelligence information can originate from a number of sources, open source or OSINT, geospatial or GEOINT, human or HUMINT, and signals or SIGINT. This last source SIGINT can be further broken down into communications or COMINT, electronic or ELINT and foreign instrumentation signals or FISINT. Also when you start dealing with these various sources another program may arise and that is the Special Access Program or SAP. SAP provides another way to restrict access control even further.

Now that I have the SCI access approved, received the security briefing and signed the Nondisclosure Agreement, how do I access this information? The only place SCI can be accessed, processed or stored is in a Sensitive Compartmented Facility or SCIF. The SCIF is a specially built facility which is constructed per the standards set by Director of National Intelligence (DNI). The standard was under the Director of Central Intelligence until passage of the Intelligence Reform and Terrorism Protection Act of 2004. One very important item to understand a SCIF is very different than a vault or closed area that is built to the Defense Security Service standards for use with collateral information. Also DSS does not inspect or certify a SCIF, inspection and certification is the responsibility of the agency which is requiring the contractor to have access to SCI, so it could be the Army, Air Force, Navy, CIA, NSA, etc. Typically a SCIF will have soundproofed walls from true floor to true ceiling, solid entry door with high security lock and access control, intrusion detection system, technical countermeasures to control radio frequency (RF) emanations inside to the SCIF especially if it is in an uncontrolled building, telephone systems that thwart electronic eavesdropping and quite a few more. You will not be permitted to take anything into a SCIF that can store, record and/or transmit digital text, digital image/video or audio data. All cell phones, laptops, cameras, pdas, usb drives, etc. are also not permitted. You are subject to search when entering or leaving a SCIF. There is a saying – Once in the SCIF, always in the SCIF, nothing can be brought into or taken out of the SCIF without the approval of the security officer. Only those personnel with SCI access are allowed unescorted access, all others must be escorted at all times and some functions may have to stop when non SCI cleared personnel are present. Any time the SCIF is unoccupied it is locked, the intrusion detection system is turned on and all materials are secured, nothing is left unprotected.

Working with SCI is a lot different then working with collateral information. It is like the starship Enterprise in “Star Trek” going from hyper drive to warp speed.

Information for this article was obtained from the unclassified DNI briefing “Welcome to SCI” on the DNI website.

Computer Security

Internet - The Top Scams of 2007

Pets, romance, and secret shoppers.

They’re each among the top ruses used by Internet scam artists in 2007, according to a comprehensive report on online crime just issued by the Internet Crime Complaint Center, or IC3.

Here’s a rundown on how these scams generally work, along with other common frauds described in the report:

Pet Scams
- You see an online (or offline) ad selling a pet and

send in your money, plus a little extra for delivery costs. But you never get the pet; the scam artist simply takes your money and runs.
- You're selling a pet. You're sent a check that's actually more than your asking price. When you ask about the overpayment, you're told it's meant for someone else who will be caring for the pet temporarily. You're asked to deposit the check and wire the difference to this other person. But the check bounces and you lose the money you sent to what turns out to be a fraudster.

Secret Shoppers and Funds Transfer Scams
- You've been hired via the web to rate your experiences while shopping or dining. You're paid by check and asked to wire a percentage of the money to a third party. Like the pet scam, the check is bad and you're out the money you sent. As part of the scam, the fraudsters often use (illegally) real logos from legitimate companies.
- While renting out a property, you're sent a check that is more than your rental fee and asked to wire the difference to someone else (are you seeing a trend here?). Or you take a job that requires you to receive money from a company and redistribute funds to affiliates via wire.

Adoption and Charity Frauds
- You get a spam e-mail that tugs on your heartstrings, asking for a pressing donation to a charity and often using the subject header, "Urgent Assistance is Needed." The name of a real charity is generally used, but the money is really going to a con artist. One set of scams in 2007, for example, used the name of a legitimate British adoption agency to ask for money for orphaned or abandoned children.

Romance Fraud
- You encounter someone in an online dating or social networking site who lives far away or in another country. That person strikes up a relationship with you and then wants to meet, but needs money to cover travel expenses. Typically, that's just the beginning—the person may end up in the hospital during the trip or get mugged and need more money, etc.

Fraud stats. The report provides a complete breakdown of statistics on Internet crime in 2007. For the year, total complaints were down slightly with 206,884 submissions, but total losses were at their highest level ever, nearly $240 million. See the report for plenty more details about victims, perpetrators, and common categories of complaints.

IC3, a joint venture of the FBI and the non-profit National White Collar Crime Center, serves as a central federal clearinghouse for all reports of Internet crime.

Logging a complaint is easy: just go to the IC3 website, click on "File a Complaint," type in the details, and hit "next." Review your information and click on "submit" when you're ready to send. The good folks at IC3 will take it from there.

Resources:
- 2007 Internet Crime Report
- National Press Release
- Internet Crime Complaint Center website

Visit the website www.lokstoogoodtobetrue.com for additional information on Internet fraud.

Also from the IC3 website

Reported Dollar Loss From Internet Crime Reaches All Time High

Washington, D.C. — According to the 2007 Internet Crime Report, the Internet Crime Complaint Center (IC3) received 206,884 complaints of crimes perpetrated over the Internet during 2007. Of the complaints received, more than 90,000 were referred to law enforcement around the nation, amounting to nearly $240 million in reported losses. This represents a $40 million increase in reported losses from complaints referred to law enforcement in 2006.

Security is a team effort!