



SECURITY NEWSLETTER

July 2010
Issue 3



JPW Security Solutions, Inc., P.O. Box 913, Hawthorne, FL 32640 Phone: 352.615.1653
E-mail: jpwsec@yahoo.com Website: www.jpwsec.com

From the Editor

Hello to all our security friends out there keeping the faith and fighting the good fight. We send our sincere thanks for all you do - especially those of you in harm's way. We hope that July finds you all well.

The last couple of months have been a pretty interesting time for our security world. We were presented with a new ISOO Directive Nr. 1 which gives us some new and specific direction relative to classification, declassification and safeguarding. In it we see some specific guidance on how to mark electronic information and some new safeguarding direction. Selected personnel were busy making suggestions to the draft new NISPOM for Industry. The OPSEC conference was rescheduled after the Tennessee floods caused the original seminar to be cancelled. We are getting a new DNI and he probably will come over to ODNI from the USD for intelligence. We had a lot of dialogue about disclosure of sensitive information in the public press (i.e., the Washington Post). The nine 2010 Industry Cogswell Award winners were announced by the DSS. The total number of OCAs was reduced by over a third thanks to our friends at the Department of State. Finally, we were told that new standards for the construction of SCIFs are on the way. Whew! We need to take a break!

I hope that all of the above activity helps you to understand that to maximize your value to your organization you need to read a lot to keep up on changes. If we want senior management support and employee buy-in for our security programs, we need to stay on top of evolving issues. You reading this newsletter is a step in the right direction - reading ISOO Directive Nr. One is probably even more important. Thank you for taking the time to peruse our little newsletter - pass it on. We would like to extend a personal

INSIDE THIS ISSUE

From the Editor	1
Who's the Lurker on the Network?	2
New SCIF Standards Imminent	2
Shame, Shame, Shame on Us	2
Cyber Security Crisis	3
2010 OPSEC Conference	3
Clearance Reform Nuggets	3
2010 James S. Cogswell Awards	4
Report Suspicious Activity	4
New Security Guidance on the Horizon	4
Halt Who Goes There?	5
Espionage Case in the News	5
Are the Good Times Really Over for Good	6
If it Doesn't Look/Sound Right - Report it	6
Outside Bad - Inside Good	7
Adjudication for a Security Clearance	7
Did You Know?	7
Original Classification Authorities and Classification Mgt	8
Public Disclosure of Sensitive or Classified Information	9
Random Thoughts for your "Things to do" List	9
Schedule of Classes	10
Secure Web Fingerprint Transmission	10
NMCIWG Newsletter	10

Contents of this newsletter represent the views and opinions of only JPW Security Solutions. Consult with your Cognizant Security Office for the "official word" on any security issue.

Please enjoy this newsletter and forward it on to at least one other security professional. I encourage you all to provide us feedback and comment at jpwnewsletter@yahoo.com and to sign up for routine electronic distribution if you are not already on our distribution list.

invitation to all of you to join us in Las Vegas for either the Security Specialist course (September) or the NISPOM course (October). Bring your quarters and perhaps your families and grow professionally and donate to the Nevada economy. Hope to see you there.....John



WHO IS THE LURKER ON THE NETWORK?

Recently, while staying at a hotel in Washington DC, I accessed their free Wi-Fi connection and was happily surfing the internet. Unsecure networks are becoming ubiquitous and can be found at hotels, the airport, sidewalk cafes, the library, and even some restaurants. These networks certainly are convenient but inherently dangerous. My computer has good security software loaded on it and it politely reminded me that there were other users on this unsecured network and that the impediments to bad guys I have installed on my secure home network are not necessarily present on this network.

I bet there are favorite close-by hotels at which visitors to your organization stay. If I was a collector for an intelligence service, and if your organization was involved in the technologies I was interested in, I think I would intentionally stay at that hotel especially during periods when I knew high-level meetings or seminars were on-going at your command or facility. I would then lurk on the free unsecured network looking for machines of interest into which I could possibly intrude and exfiltrate sensitive information.

With this in mind, we need to advise our personnel to: limit their use of these unsecure networks; disable peer-to-peer networking, file sharing, and remote access on their travel machines; ensure their operating systems have all of the newest updates installed; have good security software installed on their laptops and don't keep sensitive information on the machines they take on travel.

NEW SCIF STANDARDS IMMINENT

Intelligence Community Directive (ICD) 705 was signed by former DNI Admiral Dennis Blair and is effective May 26, 2010. The Directive states that all SCIFs shall comply with uniform security requirements and that these standards are to be promulgated no later than August 26, 2010.

SHAME, SHAME, SHAME ON US



"The environment at the base made it easy to smuggle data out. I would come in with music on a CD-RW labeled with something like 'Lady Gaga,' erase the music then write a compressed split file. No one suspected a thing and odds are they never will. I listened and lip-synced to Lady Gaga's 'Telephone' while exfiltrating possibly the largest data spillage in American history. Weak servers, weak logging, weak physical security, weak counterintelligence, inattentive signal analysis - a perfect storm"....Top Secret-cleared/SCI-indoctrinated Army SPC (35F) Bradley Manning who is in jail awaiting charges/trial for sharing Top Secret video and data files with wikileaks who then placed it on their internet web page.



"As a matter of national security and employment discipline, it is important that leakers face repercussions for improper disclosure of classified information.".....

Senator Sheldon Whitehouse (D-RI)

CYBER SECURITY CRISIS

We have all read about and perhaps even experienced cyber attacks in one form or fashion. Let there be no doubt that cyber security in our government and industrial networks is a national security and economic crisis. The DNI recently stated his concern that we have entities roaming around in our sensitive networks and we don't have a clue who they are! You can rest assured that if your agency or company has information of value that you have been hacked and probably don't even know it.

The good news is that an august group of IT experts from both government and industry agree that most cyber attacks are perpetrated via misconfigured (from a security perspective) systems - something we can mitigate with good IT hygiene. These security experts have developed a set of 20 critical security controls that, if implemented by your IT staff, should negate the efforts of 85% of the attacks that come from (unsophisticated) bad guys. These 20 guidelines can be found at <http://www.sans.org/cag/>.

The comprehensive baselines of security resulting from the implementation of these controls will be a worthwhile investment and will hopefully allow your network security folks time to develop an advanced defense against the remaining 15% (sophisticated) cyber threat that is targeting your network.

Action Item: Ensure your IT security personnel are aware of the 20 consensus audit guidelines/critical security controls.

2010 OPSEC CONFERENCE

The (rescheduled) OPSEC conference will be held September 7 – 10, 2010 at the Gaylord National Resort and Convention Center in Washington DC. Go to <http://www.iooss.gov> to register.

CLEARANCE REFORM NUGGETS

The Defense Information Systems for Security (DISS) will eventually integrate ISFD, IIRR, ENROL, DCII, JPAS, and HSPD-12 security and suitability and will become the single point of entry for DoD Security. e-Qip will be used for SF85/SF85P submissions. The government is planning to decommission JPAS starting in 2012 with completion by April 2013. JAMS will become CATS and JCAS will become the Joint Verification System (JVS). ACES is the "Automated Continuous Evaluation System" used by the DoD to check government and commercial databases in support of continuous evaluation monitoring of cleared employee behaviour.



ISFD – Industrial Security Facility Database

IIRR – Improved Investigative Records Repository

ENROL – Educational Network Registration and On-Line Learning (DSSA)

DCII – Defense Central Index of Investigations

JPAS – Joint Personnel Adjudication System

HSPD-12 – Homeland Security Presidential Directive Nr.12 (requires PIV cards)

e-QIP – Electronic Questionnaires for Investigations Processing (an OPM product)

JAMS – Joint Adjudication Management System

SWFT – Secure Web Fingerprint Transmission (digital finger prints)

CAS – Central Adjudication Tracking System

JCAS – Joint Clearance and Access Verification System

JVS – Joint Verification System

ACES – Automated Continuous Evaluation System

2010 COGSWELL AWARDS

The James S. Cogswell award is given annually by the Defense Security Service to those cleared Industry contractors that are perceived to have the most effective security programs. Out of the over 13,000 cleared contractors **only nine were selected this year** for this auspicious award. Super congratulations to the following facilities:



1. Aerospace Corporation, Albuquerque, NM
2. AMSEC, LLC/ Northrop Grumman, Virginia Beach, VA
3. Camber Corporation, Huntsville, AL
4. Honeywell Technology Solutions, Lexington Park, MD
5. L3 Services, Colorado Springs, CO
6. L3 Unmanned Systems, Easton, MD
7. Lockheed Martin, Missiles and Fire Control, Chelmsford, MA
8. Maui High Performance Computing Center, Kihei, Maui, HI
9. Northrop Grumman Information Technology, Niceville, FL



At the recent NCMS seminar, Kathy Watson told us that at the DSS counterintelligence is the number one priority. FSOs of cleared contractors are to send “suspicious activity” reports to the DSS. As a result of these reports, 45 investigations were opened in FY09 and over 100 investigations have been opened as of June 2010.

In an effort to emphasize the importance of CI reporting and to recognize those industry companies who are actively supporting the program, DSS will soon compliment the current James S. Cogswell award with a new CI award.

A reminder to Industry contractors that ISL 2010–02 requires you to report cyber intrusions that indicate actual, probable or possible espionage, sabotage, terrorism, or subversive activities directed against information systems maintained by contractors. These reports should be sent to the FBI, with a copy to DSS, **regardless of whether the system processes classified or unclassified information.**

NEW SECURITY GUIDANCE ON THE HORIZON

EO 13526 (providing direction for classifying, declassifying, and safeguarding classified information) was signed December 29, 2009 by President Obama. ISOO Directive Number one which gives us specific implementation guidance for the EO was updated June 28, 2010. Both the EO and the ISOO Directive can be found on the ISOO web page at <http://www.nara.isoo.gov>.

Meanwhile I understand that the Army regulation on Industrial Security (AR 380-49) is in its latter stages of review and revision and the NISPOM (EO implementing manual for contractors) is under review.

HALT! WHO GOES THERE?



The purpose of an intrusion detection system (IDS) is not to prevent the bad guy from entering a controlled space but instead to alert/inform the owner that the integrity of the space has been compromised. There are generally four phases to an IDS:

1. Detection (Whoa! What was that?)
2. Communication (Houston, we have a problem)
3. Assessment (Hmmm...Wonder what I should do here?)
4. Response (We're checking this out!)

Detection is the job of the sensors and contacts. The most common sensor is a PIR or "passive infrared" sensor – one that detects changes in the IR spectrum (where human bodies radiate heat energy) and does not radiate electromagnetic energy itself (passive).

The communication function is the job of the Premise Control Unit (PCU). That is the box (located in a secure area – preferably in the protected room) that normally contains the motherboard, communications module and backup batteries.

Assessment is the job of the human monitors of the IDS. They will decide how to react based on the operating procedures.

The response to the alarm is accomplished by the response force which may be on-site, a roving patrol or personnel recalled from home.

The IDS is activated to protect the spaces after normal working hours. You should test the IDS at least once per year for a Secure Room/Closed

Area and at least twice a year for a SCIF or SAPF. During the test, check the contacts on the doors, tamper alarms on your sensors and the PCU and accomplish a "4-step walk test" of the sensors to ensure they recognize anomalies/perturbations in the room when they occur. Then ensure that you fix any discrepancies and document your results. If you are a contractor, ensure your IDS is UL2050 certified and installed by a UL-certified installer.

ACTION ITEM: To learn more about IDS operations come to our next Physical Security class.

ESPIONAGE CASE IN THE NEWS



The trial of Noshir Gowadia is finally underway. Mr. Gowadia, who was instrumental to the development of IR signature suppression technology of the B-2 bomber, allegedly shared this Top Secret Air Force information with his People's Republic of China friends during six trips to China as well as contacts in Israel, Switzerland and Germany. A copy of the FBI arrest affidavit can be found here: <http://www.4law.co.il/b2.pdf>



Mark your calendars so you can attend the next NCMS Seminar June 21 - 23, 2011 in New Orleans.



ARE THE GOOD TIMES REALLY OVER FOR GOOD?

There are those who say that the best years of our country are behind us. We talk about what a mess our country is in and how other countries will soon surpass us as the world leader. I don't think this pessimistic outlook necessarily has to come to fruition. I believe we can make a difference and cause a return to what made this country great. If each of us decided to set the example and started doing what we know is right, we could start a revival of hard work, persistence, professionalism, respect, productivity, discipline and all of those characteristics of an improving society rather than one going into the toilet. I suggest we all start today to expend some energy to accomplish the following:

- Get out of debt and save 20% of what we make
- Look for new ways our agency or company can be more productive
- Help young people to appreciate the importance of saving for retirement when they are young
- Take care of parents when they get older and need us
- Work hard to get rid of bad politicians; especially those in Congress – learn the issues and vote smart – not partisan
- Create more opportunities for our subordinates
- Mentor the young hard chargers
- Use less foul and hurtful language and be kind to others
- Respect diversity and people's right to be different from us
- Give our agencies and companies the full 40 hour week of our best effort
- Use the internet appropriately at work
- Never pass up an opportunity to appreciate the efforts of our uniformed

and non-uniformed warriors and first responders

- Live honourable lives with high ethics, morals and values
- Love our kids but give them boundaries and hold them accountable
- Conserve fuel, recycle and protect the environment and wild life
- Teach our kids the importance of a good education and the value of hard work
- Become more educated ourselves so we can be more professional in our jobs

IF IT DOESN'T LOOK/SOUND RIGHT - REPORT IT

Has one of your employees been unexpectedly invited to interview for a technical job that pays twice his/her current salary? Has a foreign entity asked one of your employees to review and QC a technical paper whose subject is military-related or an export controlled technical service, data or article? Has one of your cleared employees who perhaps is a first or second generation citizen been unexpectedly invited to speak in his/her country of origin with expenses paid? Has your agency or company experienced a last minute substitution in a visiting foreign delegation?



If any of the above has been brought to your attention, perhaps this is indicative of someone up to no good and this information should be reported to your counterintelligence folks. I believe they would all say they cannot, and do not, receive too many reports. Remember, if it "just doesn't look/sound right" – report it!

OUTSIDE BAD - INSIDE GOOD



Have you ever thought about the fact that door hinges can be found on the inside of the room (allowing the door to swing in) or on the outside of a room (allowing the door to swing out). In a Secure Room/Closed Area/SCIF or SAPF which hinge installation would be problematic?

If you said the install where the hinges are on the outside, you would be right. When the hinges are on the outside, the barrel pin of the hinge can be easily removed allowing removal of the door. Plan to have your doors open in but if this is not possible, insert a set screw or spot weld the hinge so the barrel pin cannot be removed.

ADJUDICATION FOR A SECURITY CLEARANCE

There are 13 guidelines used by adjudicators to decide if an applicant is reliable, trustworthy, has full allegiance to the U.S. and thus should have access to classified information. The problem areas seen most often by adjudicators in descending order include:

- Financial
- Criminal
- Foreign influence
- Alcohol
- Drugs

Security clearance adjudication is the evaluation of information, both favorable and unfavorable, regarding the individual under consideration for

obtaining and/or retaining security clearance eligibility. The adjudicator is attempting to look at the “whole person” to decide who the individual is today. The background investigation may have uncovered some derogatory (negative) information and conversely, some mitigating (positive) information. For instance, an applicant may have been charged with DWI but successfully completed a 6-week alcohol abuse education program. The presence or absence of a particular condition or factor for or against clearance approval is not outcome determinative. I.E., the DWI does not necessarily mean the applicant will not get a clearance but on the other hand, the successful completion of the alcohol abuse program does not guarantee that access will be granted.

Adjudicators receive the following direction in the Adjudicative Guidelines: “Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security”. In other words, if there is any doubt, say no. The current goal for adjudication completions is within 20 days.

If your job description includes personnel security, you should be familiar with the content of the adjudicative guidelines. One very effective way to accomplish this goal is to attend our “Personnel Security and Suitability Adjudication” class. You can register for this class at <http://www.securityinstruction.com>.

DID YOU KNOW?



A Presidential Executive Order dated October 1, 2009 tells us that federal employees shall not engage in text messaging (a) when driving GOV, or when driving POV while on official Government business, or (b) when using electronic equipment supplied by the Government while driving.

ORIGINAL CLASSIFICATION AUTHORITIES AND CLASSIFICATION MANAGEMENT

There are currently a little over 2500 very senior government personnel who are authorized to label information as “new secrets” and to classify this information as Confidential, Secret or Top Secret. They document their classification decisions for the benefit of derivative classifiers (you and I) in documents called “Security Classification Guides” (SCG). The originators (OCAs) of these new secrets are supposed to update their SCGs at least once every five years but currently about half of the SCGs are outdated. The good news is that the President has recently ordered the agencies that generate classified information to scrub their classification management systems over the next two years. Hopefully, the result will be many updated SCGs.

Other good news is that in FY2009, two thirds of the classification decisions by the OCAs call for the newly classified information to become unclassified no later than 10 years later. The OCA can classify information for up to 25 years and has the authority to exempt HUMINT and

information about key design concepts of weapons of mass destruction from automatic declassification review when it becomes 25 years old.

Any “new” secrets must be information that is owned by, produced by, produced for or controlled by the US Government to be eligible for classification. This rules out those 11 special herbs and spices on KFC chicken and the secret formula to Coca Cola. Additionally, new secrets must fall into 8 restrictive categories detailed in paragraph 1.4 of EO 13526.

OCAs play an important part in the classification management process because all of our derivative classification decisions (if our documents are properly marked) can be traced back to their original classification decisions.

ACTION ITEM: Come to our 2-day “Information Security” course to learn more about EO 13526, OCAs, marking classified documents and the classification management process.

Testimonial: "Clear, concise, and timely instruction essential for all security professionals! Mr. Waller's credentials and enviable presentation skills ensure thorough instruction and understanding. Sidebar discussions are encouraged and provide unique learning opportunities, networking possibilities and participant cohesion."..., N.G., Batelle Corporation



Plan now to attend our "**Industrial Security for Government Personnel**" course to be presented August 18-19 at the Comfort Inn in Springfield, VA. This two-day course is designed to introduce the U.S. government industrial security specialist, Program Manager, COR or COTR to the world and concerns of the contractor. Attendees will learn what constitutes a classified contract, how to sponsor a contractor for a Facility Clearance, specific clauses that must be included in classified contracts, foreign ownership issues of concern, the National Industrial Security Program, and how to correctly complete a Contract Security Classification Specification (DD Form 254). You must be a U.S. citizen to attend.

PUBLIC DISCLOSURE OF SENSITIVE OR CLASSIFIED INFORMATION



It is often difficult for security professionals to understand their motivation but from time to time public media feels compelled to publish information they know is sensitive or even classified. The media may have noble intentions and feel strongly about government transparency but often they don't appreciate the true sensitivity of controlled information nor the impact of a compromise of classified information.

We have no control over these disclosures. However, with education, we can influence the reaction of our employees to the public disclosure so that they don't exacerbate the situation. To this end, we should periodically remind our personnel of the following:

- just because classified or sensitive information was disclosed in the public media, that does not mean it is no longer sensitive or is now unclassified
- when an employee notices a sensitive or classified public disclosure, he/she should **report this fact only to the appropriate security personnel and to those cleared officials who have a need to know** - security will then report the incident to the cognizant security office via secure means
- if the public media requests interviews with employees to discuss sensitive or classified matters or public disclosures, employees should be careful not to make any statement or comment that would confirm the accuracy or verify the classified status of the information.

Instead, they should extricate themselves from the conversation in a polite but firm manner. This interaction with the media should then be reported to security.

RANDOM THOUGHTS FOR YOUR "THINGS TO DO" LIST



- Oil your shedder regularly
- Get out of your office and visit with your cleared employees so you understand their challenges (practice security by walking around)
- Document counseling, education and training, alarm tests, self-inspections and waivers.
- Take care of the security educational needs of consultants and employees at remote locations
- Get signed receipts back from Secret and Top Secret shipments - if you don't get a receipt - where is the package?
- Aggressively protect employee private information including SF86 information
- Look for and remove public indicators that might reveal critical information (OPSEC)
- Ensure that classified documents generated by your agency/company are properly marked
- Work hard everyday to sell the idea that a strong security program is good for business, good for the agency's mission, good for senior management's careers and especially good for our troops
- Don't let a day go by without increasing your security knowledge - read, read, and read some more
- Assign only your best people to COMSEC duties

2010 SCHEDULE OF KENNETH SUDOL & ASSOCIATES CLASSES



Understanding NISPOM Requirements

Oct 18-22

Advanced Personnel Security and Suitability Adjudication

Oct 26-28

Personnel Security and Suitability Adjudication

Aug. 3-6, Sept. 14-17, and Dec. 7-10

Information Security Course

Aug 16-17

Industrial Security for Government Personnel Course

Aug 18-19

Understanding the Personnel Security Program

Sept 9-10

JCAVS/JPAS Training

Nov 18-19, and Dec 9-10

Advanced Security Studies

Dec 6-8

Physical Security and the Protection of Classified Material

Dec 9-10



NMCIWG NEWSLETTER

Are you subscribed to the New Mexico Counterintelligence Working Group Newsletter? If not, you should be. To subscribe, send an email to Scott Daughtry and in the email text include the name of your employer, your name/job title/phone number and if you are interested in having a CI representative contact you for additional cyber security or counterintelligence assistance. Scott's email address is: scott.daughtry@kirtland.af.mil

SECURE WEB FINGERPRINT TRANSMISSION



Cleared contractors use Guardian scanners to upload fingerprint files to the SWFT website. The website conducts a virus scan of the uploaded files prior to sending them to the SWFT Store and Forward server. The fingerprint files are matched against approved e-Qip submissions and automatically forwarded onto OPM and then on to the Federal Bureau of Investigations (FBI).

Contact Meredith Krar, at 561.493.7363 for more information or visit CrossMatch website: <http://www.crossmatch.com>.