WBSI
web business solutions inc.

Security

Newsletter

January 2017

Defense Security Service "Agency in Transition"

By: DSS Director, Dan Payne

"Looking ahead in 2017, it is clear change is happening in DSS. We are undertaking a fundamental change in how we do business. Where we were once focused on schedule-driven compliance, we are moving to an intelligence-led, threat-driven approach to security oversight.

We must begin by meeting the following four challenges:

First, we need to begin change now. The US is facing the most significant CI threat it has ever encountered. Our new methodology will help us counter this threat.

Second, we need to recognize that change presents a powerful opportunity for professional development and growth. The DSS transition will require everyone involved sharpening their critical thinking skills, developing solutions to a changing environment, and being open to new ways of thinking.

Third, we need to share the same vision for DSS. Our vision is to help ensure contracted capabilities, technologies, and services are delivered uncompromised.

To achieve this vision, we are developing a new methodology based on:

-- knowing the assets at each cleared facility
-- analyzing and considering threats to those assets
-- understanding business processes related to assets
-- determining vulnerabilities to assets
-- implementing countermeasures to address the threats
-- developing tailored security programs
-- conducting continuous reviews of tailored security programs
-- comprehending and articulating to our partners the impact of compromise
-- remaining in frequent contact with facility security professionals and program managers.

Finally, we formed an enterprise-wide integrated project team to best identify assets at cleared facilities and maintain and continuously update the information.

Thank you for your dedication to DSS and our important mission."

Dan Payne, Director DSS

Cyber Threats: Rapid Reporting by Industry Imperative

By: Mike Berry, Counterintelligence Directorate

While the cyber threat is universal, the cyber threats that affect cleared contractor classified and unclassified information systems are particularly acute. These threats come from foreign intelligence entities (FIE), criminal elements, insiders, and others seeking to exploit the systems. The added security surrounding classified information systems lessens but does not eliminate their susceptibility to compromise. The cyber threat, particularly from FIE, recognizes this, and focuses substantial effort to compromise unclassified systems to acquire the information or control they seek. They also seek to further their ability to identify and exploit classified systems and people with access to classified information. Moving the information to another system, such as a cloud service provider, may complicate the threat efforts but it will not prevent them. Additionally, the provider becomes an extension of the contractor's network; and thus, also subject to cyber incident reporting.

The cyber threat also targets unclassified systems at cleared companies and facilities that may have NO resident classified information. These non-possessing cleared contractors have access to information and resources valuable to the threat actor, e.g. unclassified sensitive technology, cleared personnel and the work they do, classified contract related information, and systems test/maintenance records. Whether or not the cleared contractor holds classified information, its classified systems are cyber threats targets and the contractor has the same cyber threat-reporting requirement.

The cyber threat is persistent and adaptable. It mounts continuous and prolific efforts to compromise cleared contractor systems and employees through the unclassified cyber domain, and quickly exploits the vulnerabilities and information it discovers.

Therefore, rapid and early identification and reporting of these threats and timely defensive responses are essential to ensure quick mitigation of the risks to classified contracts and information, the related sensitive technology, and cleared facilities and personnel. This reporting helps the cleared contractor and the government to curtail adversary success and preclude or minimize future occurrences at other locations.

Defense cleared contractors should report cyber threat incidents on their classified AND unclassified systems as directed by the NISPOM.

Understanding OPSEC (Operations Security)

By: DoD, Education Activity

Tips for Improving your Observation Skills

1. Mindset – take time to be aware of your surroundings. On the way from the parking lot to the front door, have you noticed how the majority of people walk to and from their cars? Odds are their head is down, staring at their phone or staring at their feet thinking of the multitude of tasks to be accomplished that day. Take the time to look and observe your environment and more importantly the people within it. Smile and look people in the eye as you pass them. Were they wearing their badge? Do you know their name? Actively searching to learn more details of your surroundings will dramatically increase your overall awareness and observation skills.

2. Sight – always be aware of your visual surroundings and study your environment. Focus on the details. Do you know the color of the person's shirt that is sitting next to your cube/office? Learning to focus on the small details will enable you to notice the bigger picture items. By knowing what is normal in your neighborhood or workplace you will be able to quickly pick up on what should and shouldn't be there.

3. Conversations – don't just hear what someone is telling you. Pay close attention and actively listen to them. Listen to the words they are saying, but more importantly their tone and body language. Try to put to memory what you have learned in conversations (e.g. first and foremost their name).

These are just small tips to help improve your observation skills. It all starts with changing your mindset and making conscious effort to be observant and aware of your surroundings.

NEW DoD HOTLINE:

Anyone may file a complaint with the DoD Hotline. While you may contact the DoD Hotline at any time, a more expeditious route towards the resolution of your problem might best be served to first CONTACT YOUR LOCAL SECURITY OR COMMAND-LEVEL IG OFFICE.

Please make note and bookmark the following website. The website allows you to select the type of complaint you wish to report as well as the method of reporting.

http://www.dodig.mil/hotline/

CONTACT US:

Holly Higgins/FSO: holly.higgins@wbsi.com

Charity DellaCamera/ALT FSO: charity@wbsi.com