WBSI
web business solutions inc.

Security Newsletter

January 2018

Adjudicative Guideline – Guideline A

By: *DoDSecurity.Blogspot*

Many are aware of the Thirteen Adjudicative Guidelines of which security clearance decisions are made. For those not aware, the security clearance process encompasses three states: *initiating* the background investigation, *maintaining* their clearance privilege, and the *continuation* process via the period reinvestigation (PR) request with background investigations, observations, and adjudication decisions. Examples of the three states: (1) when an employee is required to perform on a classified contract, the Facility Security Officer *initiates* a security clearance background investigation. (2) When an employee performs on a classified contract, their security clearance privilege is in *maintenance* mode utilizing a continuous evaluation process. (3) When a cleared employee's job requires a *continuation* of their clearance, the FSO submits a periodic reinvestigation request. These three security clearance states rely on the employee demonstrating their competency to protect classified information under the Thirteen Adjudicative Guidelines. This article is the first in a series of articles to describe each guideline.

Guideline A – Allegiance to the United States. Under Guideline A, the employee bears the burden to clearly demonstrate unquestionable loyalty to the United States. After all, they will be in possession of sensitive information that could lead to varying levels of damage to national security if compromised.

Adjudicative Guideline – Guideline A (cont.)

Under Guideline A, decisions are based on findings of disloyal activity, not on the applications words of faithfulness. There are many ways to demonstrate questionable loyalty that outweigh verbal declarations. For example, you might think your neighbor's daily flag raising ceremony is very patriotic and you may never question their loyalty. However, your discovery of their belonging to an organization sympathetic to America's enemies may change your view. In light of their questionable associations, their reciting the Pledge of Allegiance every day is a nice gesture that is outweighed by their behavior. In a security clearance investigation, these observations may cause a denial or revocation of a security clearance; no matter how much they protest their love of America. The risk that they may compromise classified information to support their potentially true allegiance is too great. An example of a Guideline A violation could be joining an anti-America or other hate group demonstrating desire to attack, overthrow, sabotage, or otherwise cause harm to the American government or just supporting those who do. This "joining" could be as involved as participating in activities, attending meetings, or just "liking" a social media group run by a foreign or domestic terrorist organization.

Identity Theft & Tax Scams

By IRS.gov

The Internal Revenue Service, state tax agencies and the tax industry, acting as the *Security Summit*, have warned tax professionals of early signs that cybercriminals already are at work as the nation's tax season approaches. Fraudsters are using a new round of emails posing as potential clients or even the IRS to trick tax practitioners into disclosing sensitive information.

The Security Summit partners encourage tax practitioners to be wary of communicating solely by email with potential or even existing clients, especially if unusual requests are made. Data breach thefts have given thieves millions of identity data points including names, addresses, Social Security numbers and email addresses. If in doubt, tax practitioners should call to confirm a client's identity.

Numerous data breaches last year mean the entire tax preparation community must be on high alert this filing season to any unusual activity. Thieves may try to leverage stolen identities to steal even more data that will allow them to better impersonate taxpayers and file fraudulent tax returns for refunds.

Identify Theft & Tax Scams

By: IRS.gov

The Security Summit has made significant strides in combatting identity theft. But cybercriminals continue to evolve and Summit partners need the help of everyone, including tax professionals and taxpayers, to continue this progress.

In recent days, tax professionals have reported numerous attempts by fraudsters to pierce their security by posing as potential clients. Crooks are using the same tactic they did last year (IR-2017-03), using phishing emails to trick tax practitioners into opening a link or attached document.

The fraudsters, posing as potential clients, send initial emails to tax practitioners. In recent days, the IRS has seen these early variations of these email schemes:

"Happy new year to you and yours. I want you to help us file our tax return this year as our previous CPA/account passed away in October. How much will this cost us?...hope to hear from you soon."

"Please kindly look into this issue: a friend of mine introduced you to me, regarding the job you did for him on his 2017 tax. I tried to reach you by phone earlier today but it was not connecting, attach is my information needed for my tax to be filed if you need any more Details please feel free to contact me as soon as possible and also send me your direct Tel-number to rich (sic) you on."

"I got your details from the directory. I would like you to help me process my tax. Please get back to me asap so I can forward my details."

If the tax practitioner responds, the fraudster will send a second email that contains either a phishing URL or an attached document that contains a phishing URL, claiming their tax data is enclosed. The fraudster wants the tax pro to click on the link or attachment and then enter their credentials. In some cases, the URL or attachment might be malicious and if clicked will download malicious software onto the tax pro's computer.

Depending on the malware involved, this scheme could give fraudsters access to the tax practitioners' secure accounts or sensitive data. It may even give the fraudster remote control of the tax professionals' computers.

The IRS also has received recent reports of fraudsters again posing as IRS e-Services, asking tax pros to sign into their accounts and providing a disguised link.

Identify Theft & Tax Scams

By IRS.ov

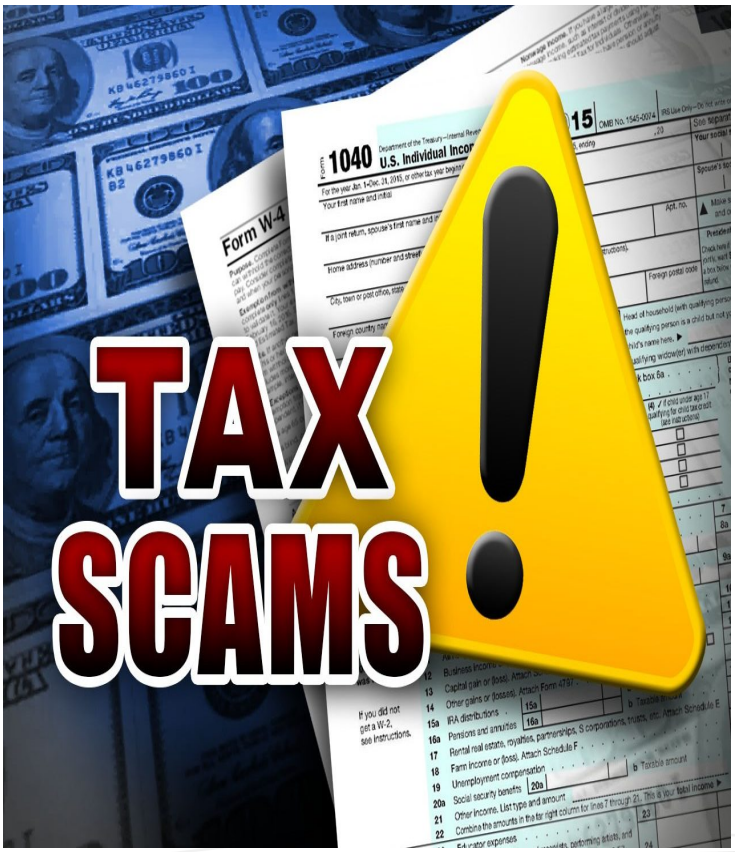
The link, however, sends tax pros to a fake e-Services site that steals their usernames and passwords.

This type of scam is one of the reasons the IRS has moved e-Services to the more secure identity-proofing process called Secure Access. It is important that all e-Services account holders upgrade their accounts to this more rigorous authentication process. E-Services account holders who have not updated their accounts should do so immediately. See https://www.irs.gov/individuals/important-update-about-your-eservices-account

Tax practitioners receiving emails from fraudsters posing as the IRS, or even their tax software provider, should go directly to the main website, such as IRS.gov, rather than opening any links or attachments. Forward attempted phishing emails to phishing@irs.gov. Remember, the IRS does not send unsolicited emails.

For additional tips, tax professionals should review the Summit partners' campaign:

https://www.irs.gov/e-file-providers/dont-take-the-bait



QUESTIONS?

PLEASE CONTACT US!

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

Charity DellaCamera/ALT FSO:
charity@wbsi.com