UNCLASSIFIED

Cyber Domain Situational Awareness

1-Feb-17

PUBLIC SECTOR

- **FEDERAL AGENCIES WARNED OF CYBER ESPIONAGE COMING FROM THEIR LANDLORDS**

Source: Fedscoop

According to a GAO report, 26 FBI, DHS, Secret Service, and DEA offices are based in buildings owned by foreign firms. Of these 26 buildings, 22 are owned by entities licensed in non-NATO countries. Based on this information, the U.S. Committee on Foreign Investment & tenant agencies have concluded that these buildings could present security risks, such as espionage & unauthorized cyber & physical access.

PRIVATE SECTOR

- **GMAIL WILL STOP ALLOWING JAVASCRIPT (.JS) FILE ATTACHMENTS STARTING FEBRUARY 13, 2017**

Source: Security Affairs

Google recently announced that their Gmail service will soon begin blocking the attachment of JavaScript files to emails due to security concerns. Other potentially malicious file types, i.e. .exe, .sys, .bat, .com, .vbs, and .cmd files are already blocked by the email service. Google suggests that users who need to share these file types do so through Google Drive, Cloud Storage, or another online storage service.

PERSONAL COMPUTING

- **31 MODELS OF NETGEAR ROUTERS FOUND VULNERABLE; COULD BE HACKED TO FORM BOTNET**

Source: SC Magazine

New vulnerabilities have been discovered in 31 models of Netgear routers that could allow hackers to take over devices. The flaws could allow an attacker to discover or bypass any password on a Netgear router. Consequently, the hacker would then have complete control of the router and be able to change configurations.

***MITIGATION STRATEGY**: Users should routinely check for & install software & firmware updates to ensure their devices remain secure.*

SECURITY AWARENESS TIP OF THE DAY

- **YOUR CHILDREN MAY PUT THEMSELVES AT RISK BY SHARING PERSONAL INFORMATION ONLINE. ALWAYS USE PARENTAL CONTROLS.**

Children could potentially compromise their identities by sharing personal information with strangers, such as their name, age, or even their address. Even something as small as a name and town could potentially be used to identify your child. Always turn on parental controls on any device your children use that can connect to the Internet.

Source: Inspired eLearning