Office of Environment, Health, Safety and Security
Operating Experience Level 3

OE-3: 2019-01 April 2019

Electronic Devices Pose Security Risks

PURPOSE

This Operating Experience Level 3 (OE-3) document provides information about some security risks posed by electronic devices that enter Department of Energy (DOE) facilities. These items have the potential to be used to record or transmit information without authorization. Some electronic devices have features that may be used to extract information with or without the user's knowledge. Examples include recording equipment (audio, video, optical, or data), electronic equipment with a data exchange port capable of being connected to automated information system equipment, cell phones, radio frequency transmitting equipment, and computers and associated media. Everyone should be aware of the security risks posed by these devices and should understand and adhere to applicable security plan requirements to mitigate those risks.

BACKGROUND

In early 2019, a security flaw was discovered in Apple's video-calling software, FaceTime, which allowed people to eavesdrop on iPhone users. The vulnerability enabled users to hear audio and see video of the person they were calling even if the person did not accept the call. This exposed all Apple iPhone users to eavesdropping, and potential unauthorized and unknown audio and video recording. While much media attention on this discovery has focused on privacy right infringement, the counterintelligence implications bear additional consideration.

There have been instances around the DOE complex where individuals unintentionally became insider threats by introducing these types of electronic devices into secure areas. In some cases, these incidents were precipitated by a change in routine that distracted individuals from performing their normal personal inventory before entering secure areas.

These incidents highlight the importance of consistent adherence to protection program operations in order to protect national security interests. As the Internet of Things expands into wearable devices and other personal electronic devices with data recording and/or transmitting capabilities, all DOE employees must maintain control of these items and understand the capabilities and potential vulnerabilities that they introduce into the workplace.

DISCUSSION

DOE employees should be aware of the capabilities and vulnerabilities of all electronic devices that they bring onto DOE sites, and to understand what is considered to be a controlled article. As our technological capabilities expand into wearable devices and other products capable of transmitting and collecting data, it becomes more difficult to remain aware of these items as we travel to and from work and between worksites. Maintaining a personal inventory of controlled items is necessary for preventing security vulnerabilities that could create unintentional insider threats. Many electronic devices are controlled articles. These include but are not limited to:

- cell phones,
- personal digital assistants,
- laptop computers,
- music players (iPods, mp3)
- e-book readers,
- tablets,
- bluetooth earpieces/headsets,
- wearable fitness devices,
- wearable health/medical devices,
- anything labeled “smart,” to include: watches, glasses, rings, televisions and other appliances, light bulbs, and,
- anything that connects to the internet.

Electronic devices can be activated without the users’ knowledge, including cameras, microphones, and apps that track and record a user’s movements, calls, and activities. These devices can potentially transmit out any information or data collected wired or wirelessly without the user knowledge to anywhere in the world. Many digital cameras, including those on smartphones, automatically capture geographical information in addition to a photograph/video. This is called ‘geotagging.’ This data can be retrieved and used to determine a user’s location, time, dates and establish patterns of travel. Microphones can be activated and used to record conversations and other acoustical information that can be analyzed and compromise information. Also, some smartphones and wearable devices have motion sensors that can detect minute vibrations; these can be analyzed with algorithms to decipher keystrokes. Any of this data can be collected and transmitted (wired or wirelessly) to adversaries without a user’s knowledge. The electromagnetic emissions from wireless devices can put nearby information systems at risk of compromise also.

Across the DOE complex, sites exercise their authority to create and enforce security rules that may differ from site to site, based on the unique nature of operations within their respective sites. Workers who travel to various sites or away from their ‘home’ site must check with a security professional to understand any differences in security requirements between the sites, and should anticipate and manage their use of personal electronic devices appropriately while on travel.

RECOMMENDATIONS

To reduce the risk of becoming an unintentional insider threat, it is recommended that DOE employees:

- Know the capabilities and vulnerabilities of the devices they are bringing onto a DOE facility. The more knowledgeable employees are about their devices, the better off they will be!
- Understand and abide by all relevant security program operations at the worksite.
- Contact security specialists prior to travelling between worksites, to prepare for differences in security requirements for other sites.
- Consider turning off data transmission services before entering a DOE worksite.
- Consider setting an alarm for the approximate time of arrival at the worksite, as a reminder to make any necessary changes prior to entering the worksite (for example, turning off location settings or data transmission, or removing wearable technology).
- Maintain a personal inventory of controlled articles to support compliance with security requirements.

CONCLUSION

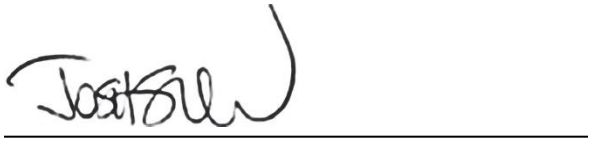
Possession of cell phones, wearable devices, and other electronics at DOE worksites poses a risk of unintentional security breaches. It is necessary for DOE employees to understand the capabilities of their technological devices and to comply with all security program requirements for controlled articles to reduce this risk.

REFERENCES

DOE O 473.3A. *Protection Program Operations*.

Questions regarding this OE-3 document can be directed to Ross Natoli at 202-586-1336 or ross.natoli@hq.doe.gov.

This OE-3 document requires no follow-up report or written response.



Josh Silverman
Director
Office of Environmental Protection and
ES&H Reporting
Office of Environment, Health, Safety and Security