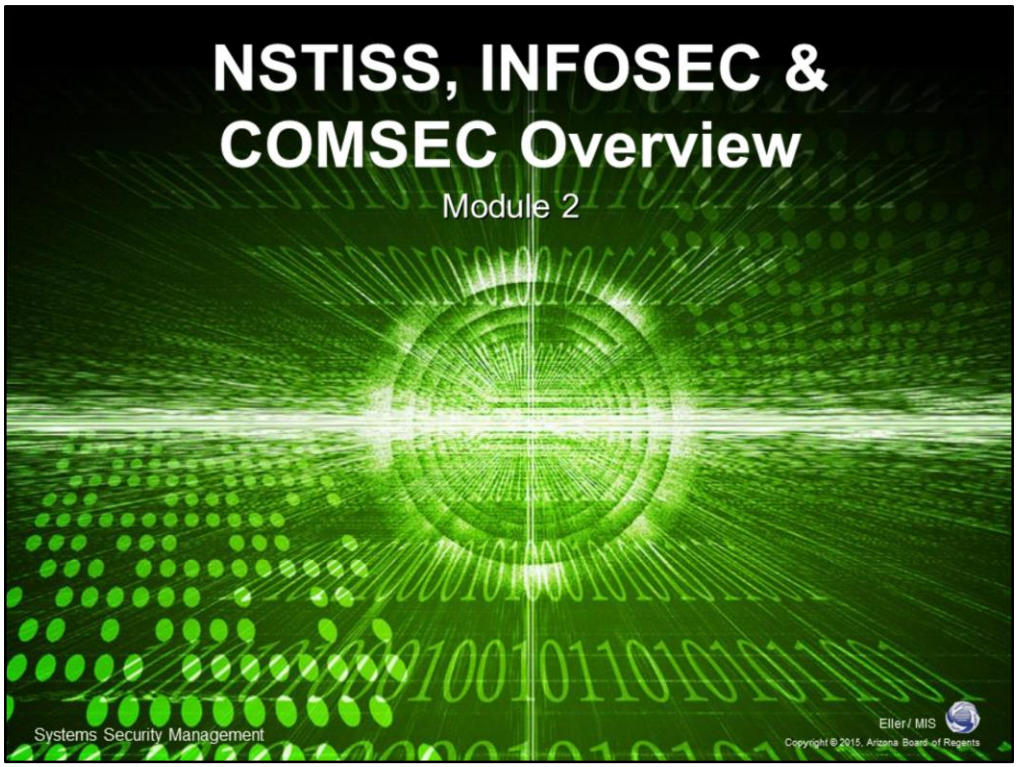
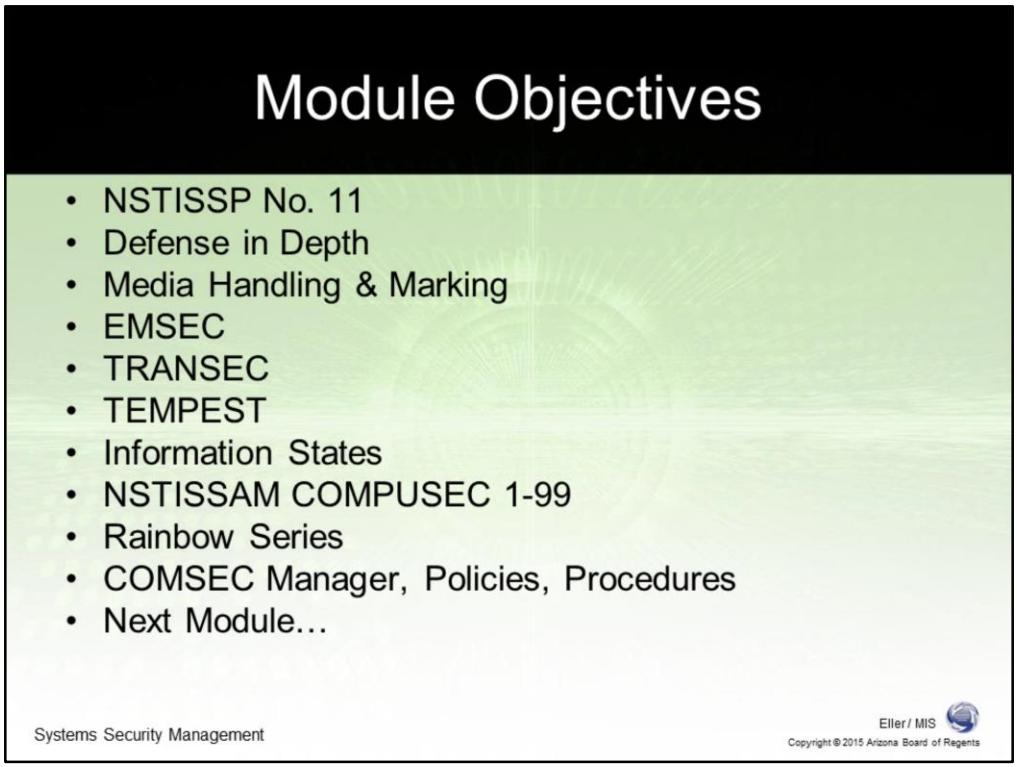
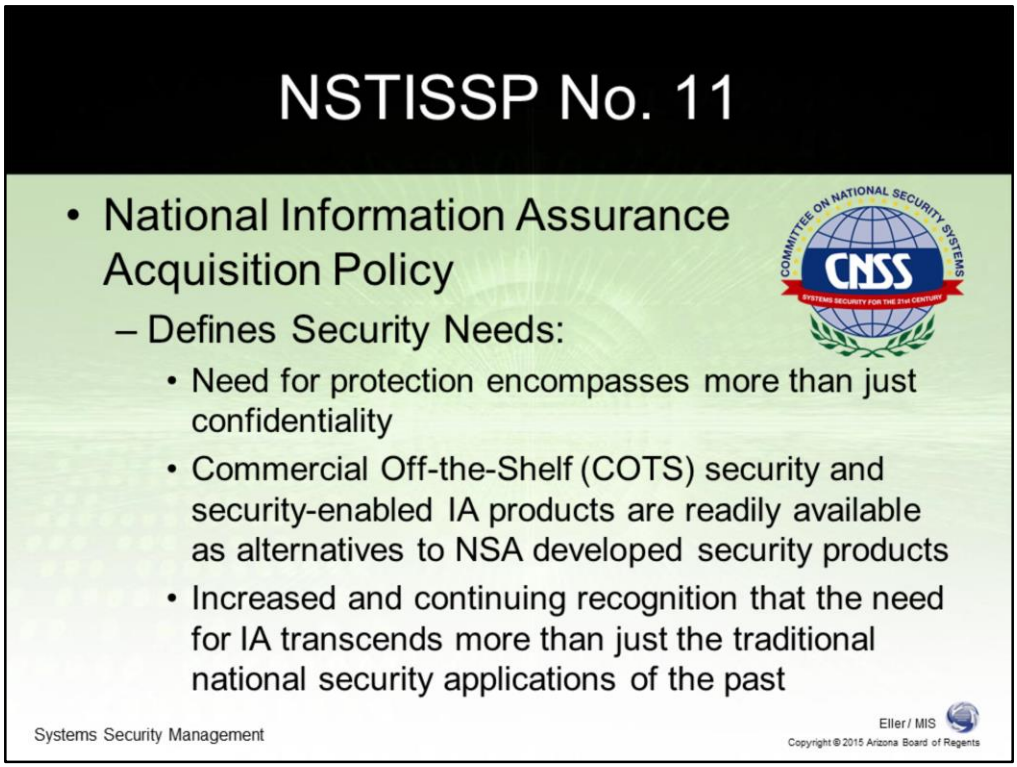

NSTISS, INFOSEC &
COMSEC Overview
Module 2
Systems Security Management
Eller / MIS
Copyright © 2015, Arizona Board of Regents



By the end of this module, you should have a clear understanding of:

•What NSTISSP No. 11 is and why it is important.
•What defense in depth is and how it is used by government.
•How to use backup media and how it should be marked to ensure proper handling.
•What emission security is and why it is important to provide adequate defense.
•What transmission security is and why it is important to provide adequate defense.
•What the TEMPEST program is and how and why it was created.
•What the different information states are and why they can be vulnerable to attack.
•What is contained within the NSTISSAM COMPUSEC 1-99 memorandum.
•What the rainbow series is and how it can be used.
•A description of the position of COMSEC Manager, including the appropriate policies and procedures to be followed.



What is the NSTISSP No. 11?

The National Security and Telecommunications Information Systems Security Policy number 11 describes the United States' National Information Assurance Acquisition Policy. This policy was written with the understanding that it may not always be possible for the government to develop its own hardware and software solutions that meet specific needs. So, this means the government will, at times, need to purchase software and applications from third party developers. These applications must adhere to the government's Information Assurance policies, so this policy was created to guide government agencies during the evaluation and purchasing process.

In order to ensure the security and assurance of information stored within third party applications, government agencies must refer to the NSTISSP #11 policy. This policy defines the following specific security needs:

The Need for Protection

The need for protection against those who would try to access the system illicitly involves more than simple confidentiality. Applications must adhere to security policies defined in NSTISSP #11 in order to protect the viability of the information stored within, whether or not the application is used to contain sensitive information.

Commercial Off-the-Shelf Products

Over the past decade, third party applications developers have been creating commercial software designed to be sold in stores and online. Many of these products have been developed with security or information assurance in-mind so they may be purchased and used for government purposes. Many of these types of software meet the NSA's requirements for information assurance as defined in NSTISSP #11.

Recognition of the Need for IA

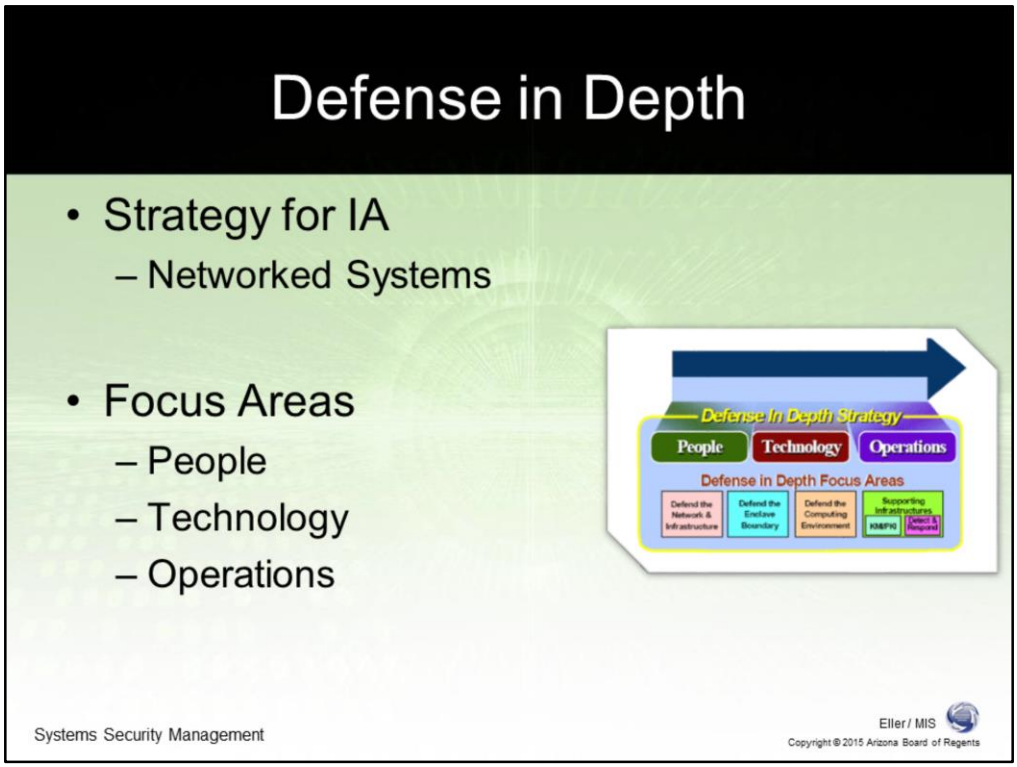
Information assurance has become increasingly important for any and all applications which allow users to store, transmit, and manipulate data and information. This is even more important now that access to applications can be accomplished from anywhere in the world through an Internet connection. Open access to applications over the Internet provides a unique opportunity for attackers to find and try to breach an information system without adequate protection in-place; therefore, the addition of IA concepts and policies into third party applications has made it easier for government agencies to adopt these applications.

Commercial Off-the-Shelf Information Technology Products

COTS IT products need to be evaluated by the agency or department needing them. This evaluation is necessary not only to ensure the system does what is needed, it is also necessary to ensure all of the appropriate IA security measures are available and working properly. COTS products are required to come from an accredited commercial laboratory, meaning the company and its products must be accredited by the National Institute for Science and Technology for IA compliance. The important thing to remember about COTS products is that Information Assurance is a requirement for their adoption.

What happens if no accredited product meets the need?

In the event that a COTS IT product is needed and one with accreditation cannot be found that meets the needs of the agency or department, then the agency or department can petition for a deferred compliance authorization. This authorization must be granted by the accrediting body and additional steps must be taken to make the system as secure as possible. “A Deferred Compliance Authorization (DCA) is a formal approval by an authorized official to defer compliance with the requirements of a national IA policy for a specified period of time, normally not to exceed more than one calendar year” (National Security Agency, 2009).



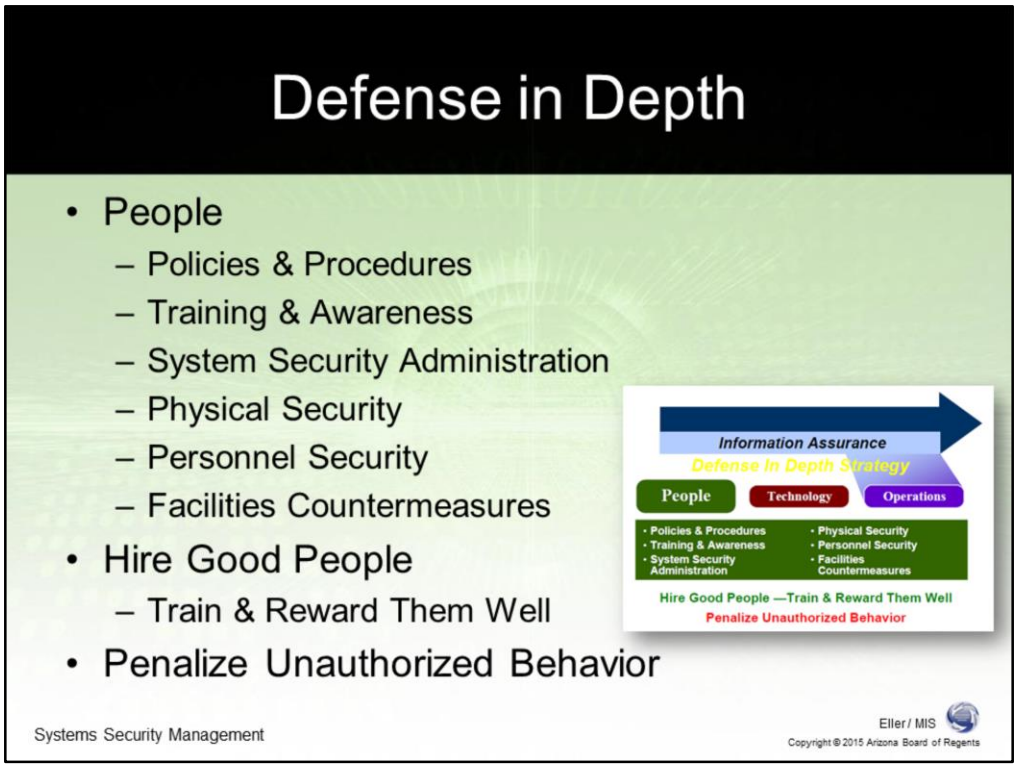
What is Defense in Depth?

Defense in Depth is an IA strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of networks. In other words, a defense in depth strategy looks to provide security and information assurance through effective use of people, technology, and operations. The primary idea with defense in depth is to make a potential target less advantageous by increasing the costs for attackers due to the layered nature of the strategy.

Defense in Depth Strategy Focus Areas

There are three different areas where Defense in Depth focuses in order to create a solid strategy. These areas are:

- People
- Technology
- Operations

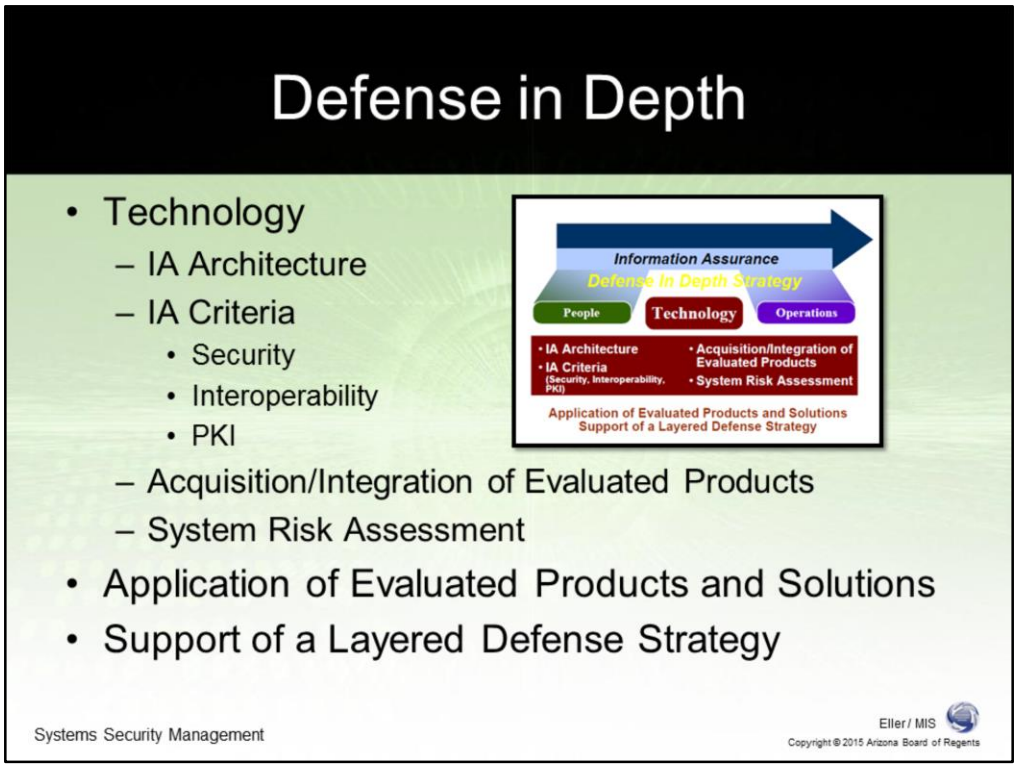


Defense in Depth: The People Aspect

People make up the organization, and as such, they will be doing the day-to-day work the organization needs. This includes accessing and manipulating data from information systems on the network. In order to ensure the security of the data on the network and work towards providing a defense in depth solution, there are several areas that need to be addressed.

- **Policies & Procedures** – Having solid policies and procedures in-place regarding information security will provide the basis for defense in depth.
- **Training & Awareness** – Once policies and procedures have been created, employees will need to be trained in the use of the information systems and made aware of their responsibilities with regard to ensuring the security of the organization's information.
- **System Security Administration** – System Administrators will need to be fully trained in the best practices for securing the information on the network. This is because it will be the SysAdmin who will be responsible for enforcing the information security policies.
- **Physical Security** – Sensitive equipment should be housed in secured rooms, using some kind of locking mechanism to keep those who are unauthorized from accessing the systems from having physical access. Some organizations may need to hire security personnel to ensure the physical security of equipment.
- **Personnel Security** – Another layer to the people equation is to ensure that employees only have access to resources necessary to perform their job duties (known as "least privilege"), along with separation of access and mandatory vacations. The HR department should also conduct background checks on employees with access to sensitive information.
- **Facilities Countermeasures** – Having good people working for the company is not enough, those personnel trusted with information security responsibilities will need to fully understand any weaknesses that may exist and how to employ countermeasures to prevent unauthorized access. Threats to the building may include compromised HVAC controls (servers need to be kept at a cool, constant temperature, otherwise damage may occur, thus affecting system availability), electrical anomalies (electronic locking mechanisms may be compromised in the event of an outage), and specialized fire suppression for datacenters and server rooms to ensure systems are protected as much as possible in the event of a fire.

The bottom line with a defense in depth strategy when referring to people is if you hire good people who are trained and rewarded well, they will be more loyal to their employer and will perform at or above expectations. In the event an employee violates security policies it will be important to penalize the unauthorized behavior in some manner appropriate to the severity of the security incident.

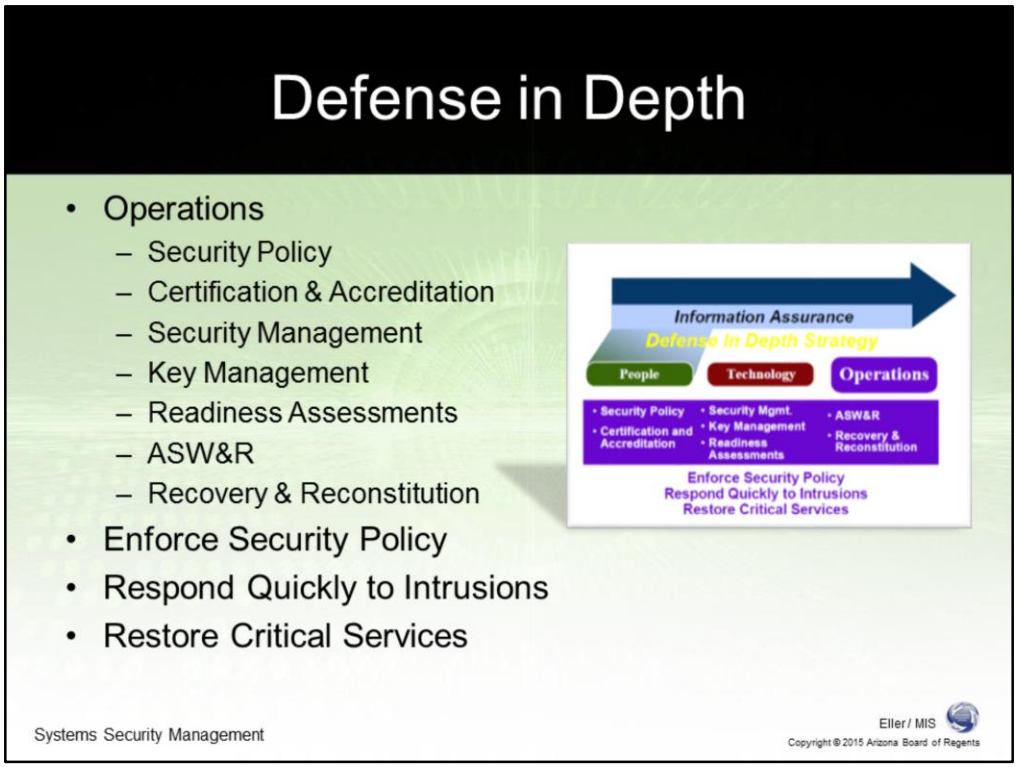


Defense in Depth: The Technology Aspect

Technology is the core by which information is shared, stored, and processed within an organization. Information security requires the use of technology in order to secure a network and information systems. Some technology aspects include the following:

- **IA Architecture** – When deploying a defense in depth strategy, the organization needs to ensure the system and network architecture has been designed using information assurance principles.
- **IA Criteria** – During the design phase for using technology, the organization needs to address the information assurance criteria of security, interoperability, and the public key infrastructure (or PKI). Adopting sound security policies that ensure sensitive information is kept from prying eyes without affecting employee's abilities to do their work is critical to the success of the organization. Adopting the use of a PKI will help to ensure the data used is transmitted securely using encryption and digital signatures to verify the file was not altered by a third party.
- **Acquisition/Integration of Evaluated Products** – It will not be possible for most organizations, especially government agencies, to develop the different software products needed. This will necessitate the purchase or licensing of third party products. These products will need to be thoroughly evaluated for IA before acquisition and adoption.
- **System Risk Assessment** – Before the organization begins to use new information systems, they must be put through a rigorous system risk assessment in order to determine vulnerabilities and provide management with the information necessary to make mitigation decisions. These assessments should be performed on a regular basis to ensure systems remain secure.

A technology strategy for Defense in Depth will involve the application of evaluated products and solutions designed to provide information assurance. Technology strategies are usually deployed in support of an overall layered defense strategy.



Defense in Depth: The Operations Aspect

Operations plays a huge role in information security and a defense in depth strategy. When it comes to the operations aspect there are a number of areas that need to be addressed.

- **Security Policy** – Solid security policies will form the backbone of the defense strategy.
- **Certification & Accreditation** – Information systems using IA in Government will need to be certified and accredited in order to ensure IA.
- **Security Management** – Managing the overall security picture within the organization includes installing security patches, virus updates, and maintaining access control lists for buildings and firewalls, etc.
- **Key Management** – Using a PKI will require technical management by the SysAdmin and his or her team in order to ensure all data is transmitted and stored securely.
- **Readiness Assessments** – Understanding the organization's current ability to withstand a cyber attack is vital to a defense in depth strategy. This includes conducting vulnerability assessments, penetration tests, and web application testing.
- **Attack Sensing, Warning and Response (ASW&R)** – Having the technology, people, and operations ability to detect attacks when they happen and respond accordingly. The military refers to this response process as an OODA loop, a term coined by a fighter pilot in the 60s. OODA stands for the decision cycle of observe, orient, decide, and act. This is a key framework for Incident Response, if you can perform that loop faster than your opponent, you will win the fight (Los, 2012).
- **Recovery & Reconstitution** – In the event an attack is successful, or just that technology has failed, the organization will need to have the equipment, software, policies, and people in-place and ready to recover the data and failed system(s).

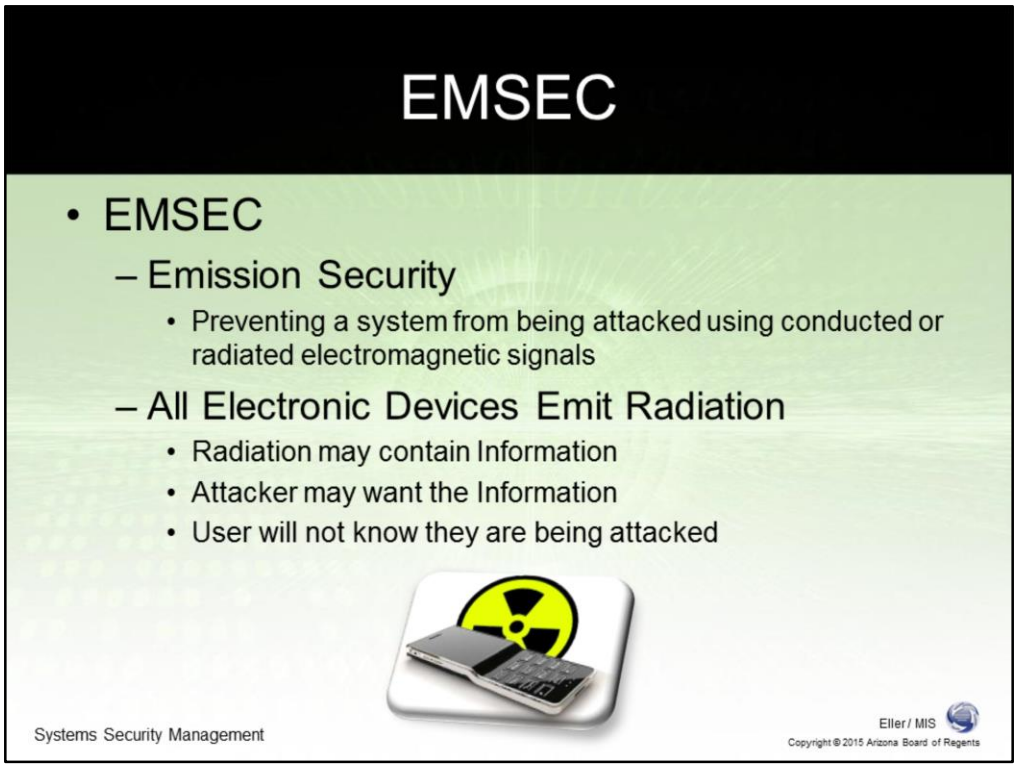
An operations strategy for defense in depth is concerned with enforcing security policies, responding quickly to any and all intrusions, and restoring critical services.

Media Handling and Marking

When using electronic media for storing files and backups, the question of how the media should be handled and marked comes to the forefront. Electronic media should be marked in a manner consistent with an organization's labeling policies. From a security standpoint it is not recommended the media be labeled with specific information about what is contained on the media. Instead the label should be generic enough to be useless if the media is intercepted, yet understandable enough for the SysAdmin to know what it contains.

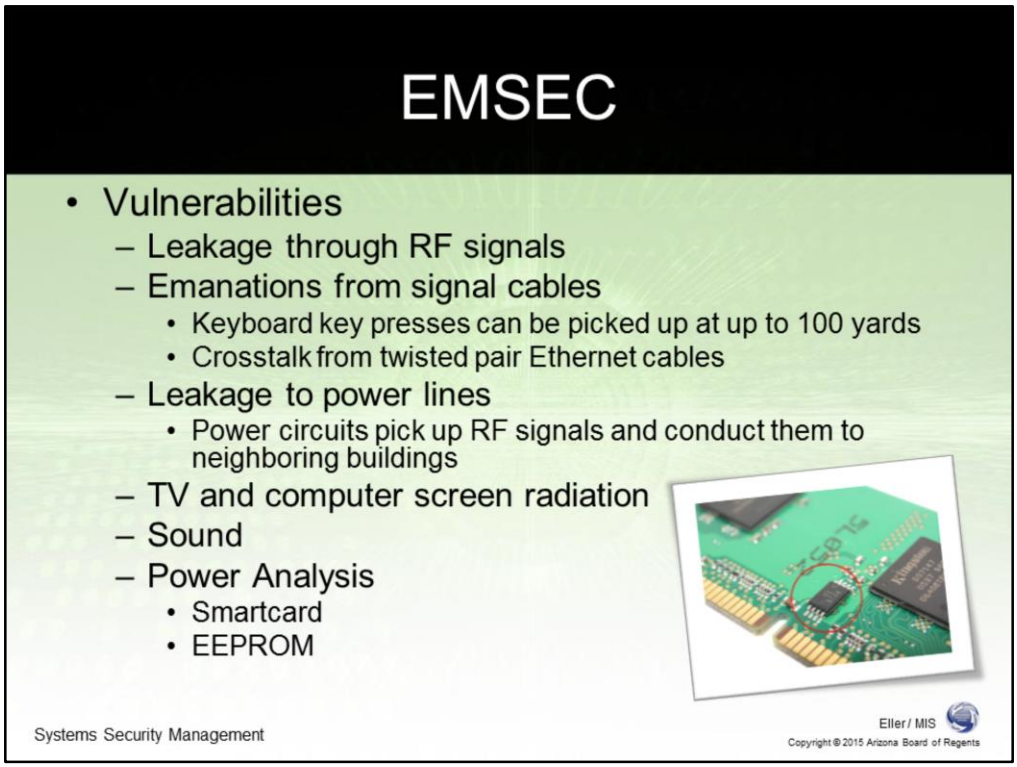
Reuse of media is also a concern. How many times should electronic media be reused before its integrity is suspect? The answer depends on the type of media and is a topic we will discuss in Module 5.

The final aspect to media handling involves media destruction policies. How electronic media is destroyed depends entirely on the type of media used. CDs and DVDs can be physically destroyed by scratching the surface and snapping the discs. Tapes are a magnetic media which can be destroyed by using strong magnets to render the data undecipherable. With hard drives, it is recommended they are formatted using a Department of Defense formatting standard which writes random data bits to the hard drive a minimum of 7 times.



EMSEC

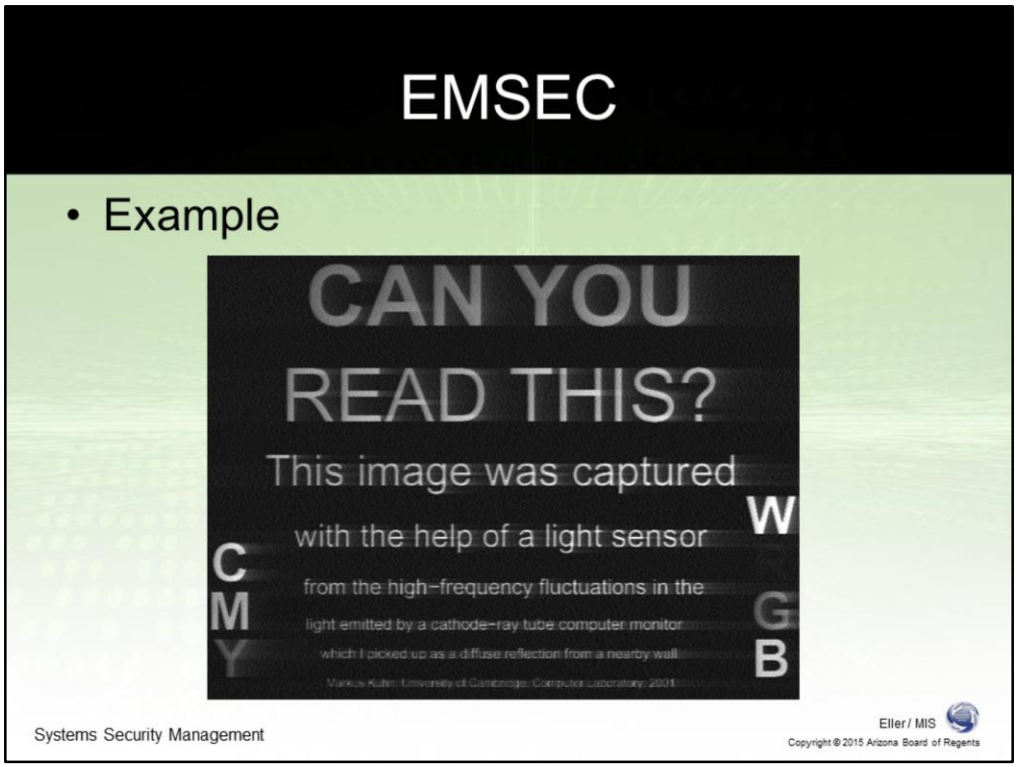
Emission Security, or EMSEC, is a technique designed to prevent a system from being attacked using conducted or radiated electromagnetic signals. It is important to understand that all electronic devices emit some sort of radiation and that radiation may contain information. The information contained within the radiation may be desirable to an attacker, and since the device is emitting this information without user intervention, the user will not know they have been attacked.



EMSEC (continued)

There are a number of ways in which electronic devices are vulnerable to an emission attack. These vulnerabilities can include:

- **Leakage through RF signals**
- **Emanations from signal cables** – For example, keyboard key presses can be picked up at up to 100 yards. Another concern is crosstalk from twisted pair Ethernet cables that can be intercepted along the wire.
- **Leakage to power lines** – Power circuits pick up RF signals and conduct them to neighboring buildings
- **TV and computer screen radiation**
- **Sound**
- **Power Analysis** – Including Smartcards and EEPROM.

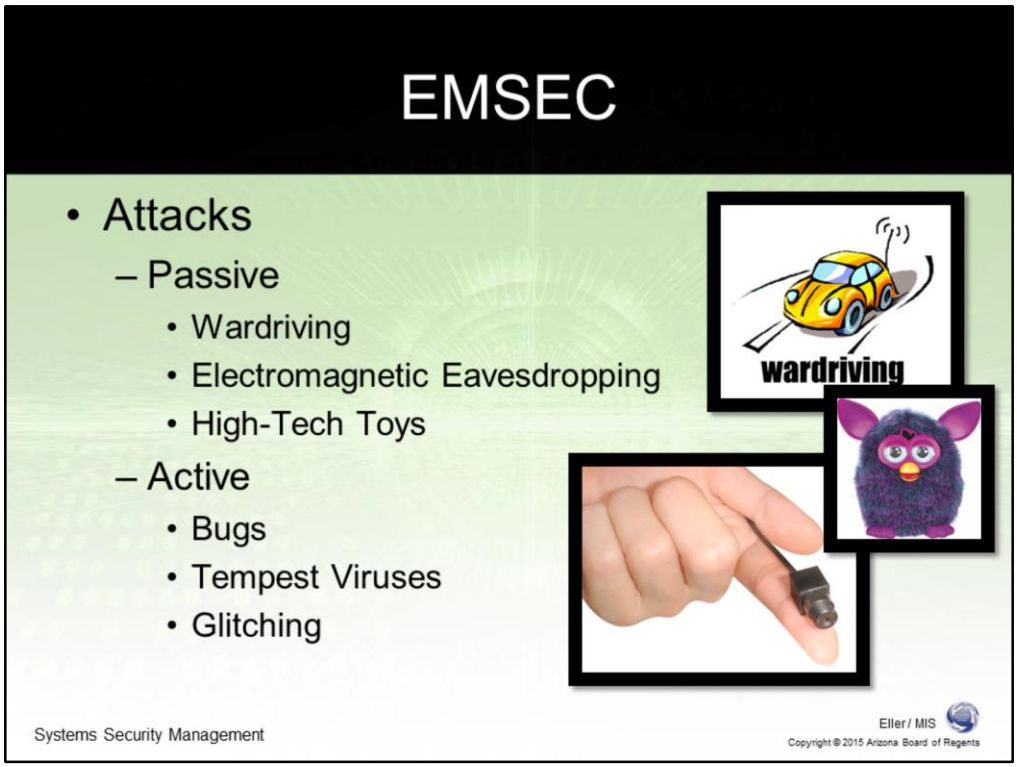


EMSEC (continued)

Here is an example of an image that was recorded from a cathode-ray tube monitor at the University of Cambridge Computer Laboratory in 2001. The monitor had this simple text:

Can you read this? This image was captured with the help of a light sensor from the high-frequency fluctuations in the light emitted by a cathode-ray tube computer monitor which I picked up as a diffuse reflection from a nearby wall.

Just imagine, if this clear of an image could be picked up off a nearby wall from a monitor, then even facing a monitor away from a window would not be enough protection to prevent someone from still being able to capture the information off the screen. This is scary stuff, especially when it comes to information security and information assurance.



EMSEC (continued)

There are a number of different possible ways to attack systems using emissions, including both passive and active attacks. Some examples of passive emission attacks include:

Wardriving - The act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable device. This is something easy for anyone to do, just take your laptop or even your iOS or Android device and have it search for wireless networks in the area. How many do you see that are not secured?

Electromagnetic Eavesdropping – This is the technique, known as Van Eck phreaking, used in the previous example with the monitor image off the nearby wall. Remember, all electronic devices emit some radiation and electromagnetic eavesdropping techniques can be used to glean information from this radiation.

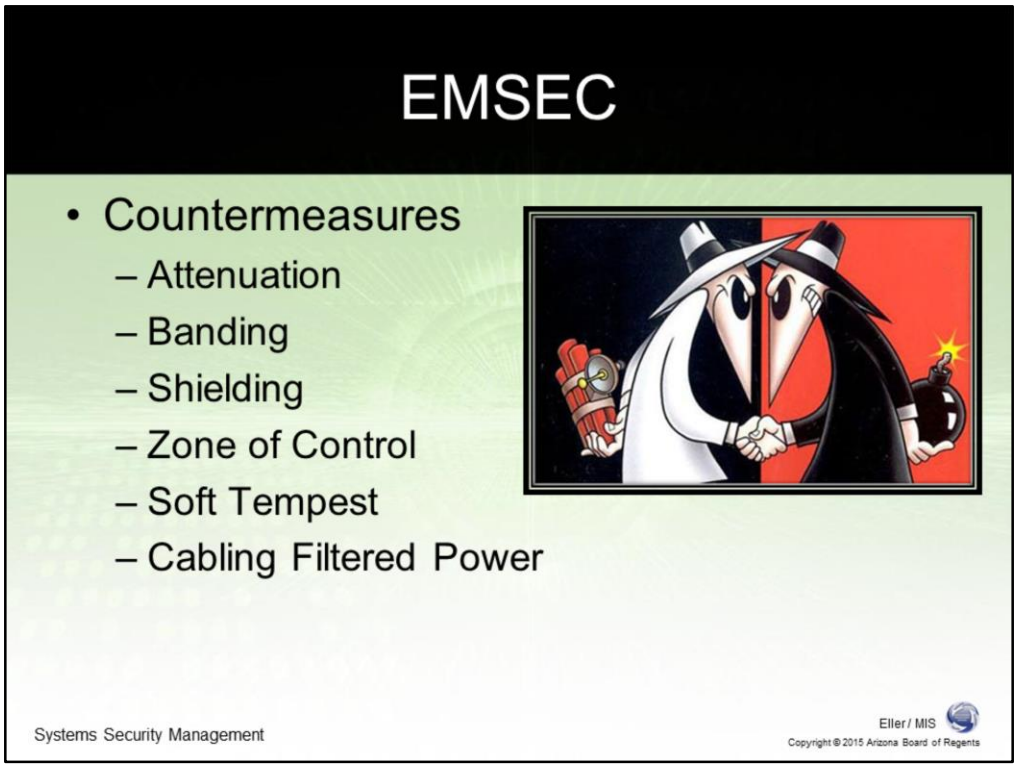
High-Tech Toys – Many high-tech toys are capable of being used in a passive attack. Since a passive attack is mostly about gathering information without deliberately making a connection with a specific system, any device with a wireless network connection or scanning ability can be used in passive emission attacks. In 1999, the NSA actually banned the hugely popular Furby toys, labeling them as a “threat to national security”, despite the toys not being able to actually record sound. This was due to wild rumors that the Furbys could “hear” their owners and repeat things they heard at random times (Mancini, 2014).

Some examples of active emission attacks include:

Bugs – Bugs have been used for years by law enforcement, governments, and sometimes for less than legal purposes by criminals, for spying on conversations.

Tempest Viruses – A virus infects a computer and makes it transmit secret data to a radio receiver hidden nearby , often through playing a little tune.

Glitching – Technique used to disrupt the ability to use a device.



EMSEC (continued)

There are a number of methods for countering emission attacks. Some of these methods include:

- **Attenuation** - This reduces the signal strength during transmission which decreases the radiation perimeter. An attacker needs to get closer to the source, which comes with a greater risk of being caught.
- **Banding** – Restricting the information to be in a specific band of frequencies forces the attacker to find out which band of frequencies to scan
- **Shielding** – Electromagnetic shielding can be installed, something like double-pane windows can be installed in order to prevent laser microphones from working.
- **Zone of Control** – Place systems that display and manipulate sensitive information in specific locations that are away from potential sources of attack.
- **Soft Tempest** – Software techniques used to filter, mask, or render incomprehensible information bearing electromagnetic emanations from computer systems.
- **Cabling Filtered Power** – One should filter cable and power supply noise in order to suppresses the conducted leakage.

TRANSEC

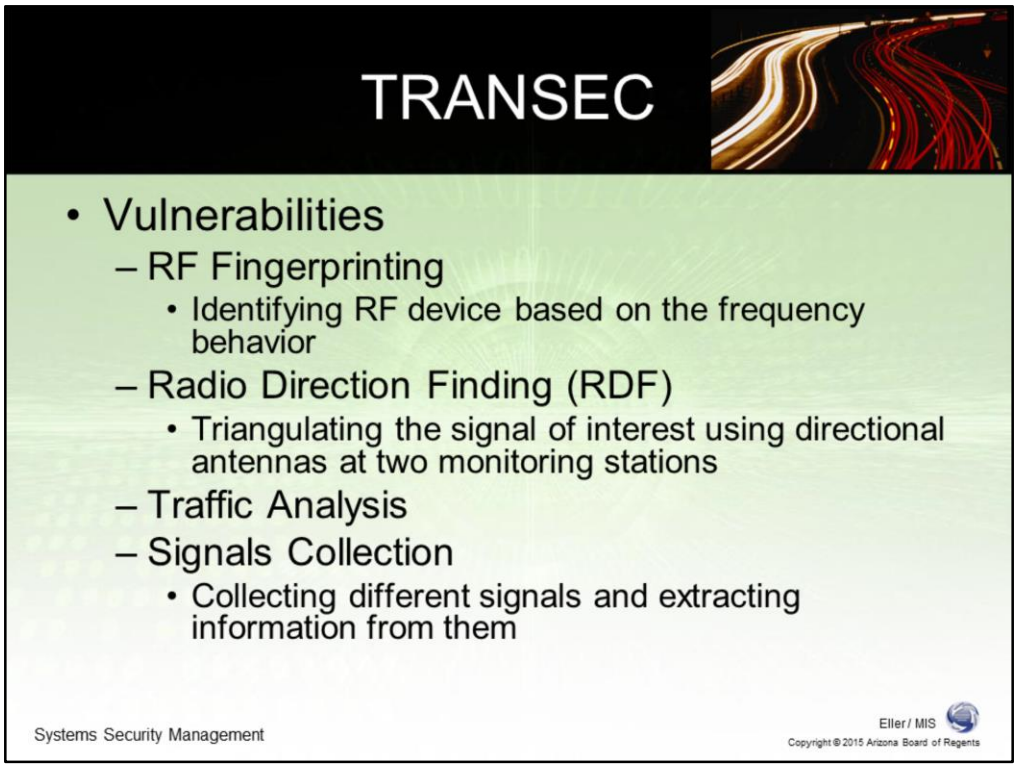
- TRANSEC
  - Transmission Security
    - Preventing data from being attacked or intercepted during transmission
  - The Need for TRANSEC
    - Information needs to be shared
    - Must be transmitted over long distances
    - Attacker may want to intercept the information while in transit

Systems Security Management

Eller / MIS

TRANSEC

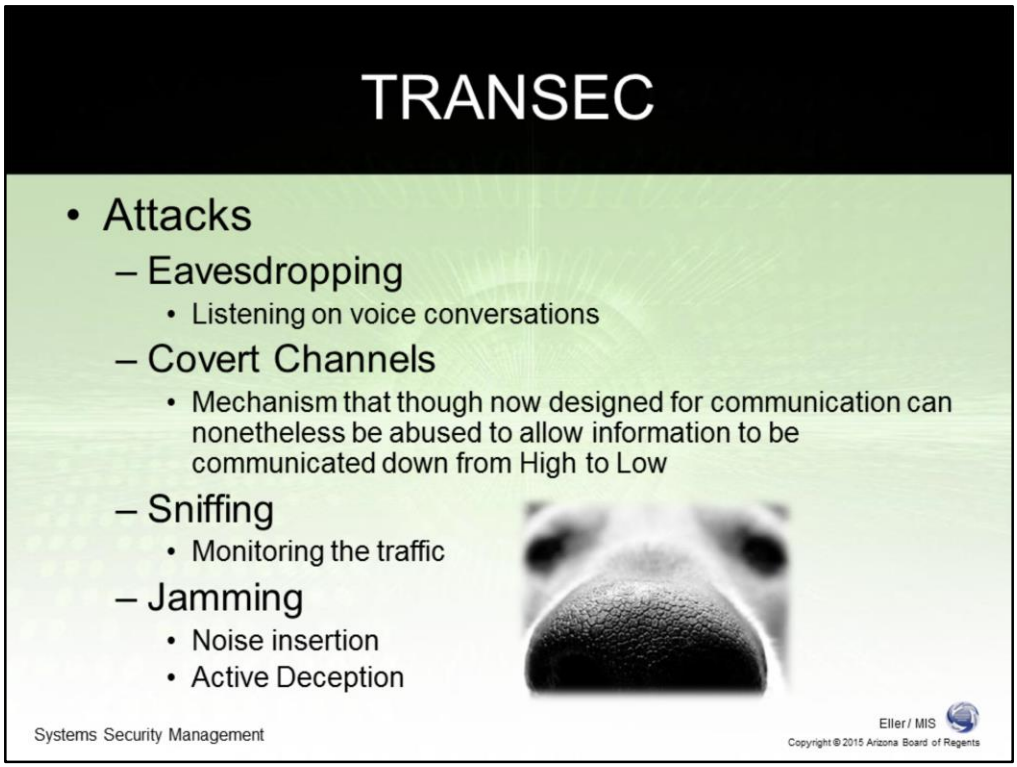
Transmission security, or TRANSEC, is a technique for preventing data from being attacked or intercepted during transmission. TRANSEC is needed simply because information needs to be shared. In some cases information needs to be transmitted over long distances, and an attacker may want to intercept the information while it is in transit.



TRANSEC (continued)

There are a number of vulnerabilities in data transmissions that an attacker can exploit including:

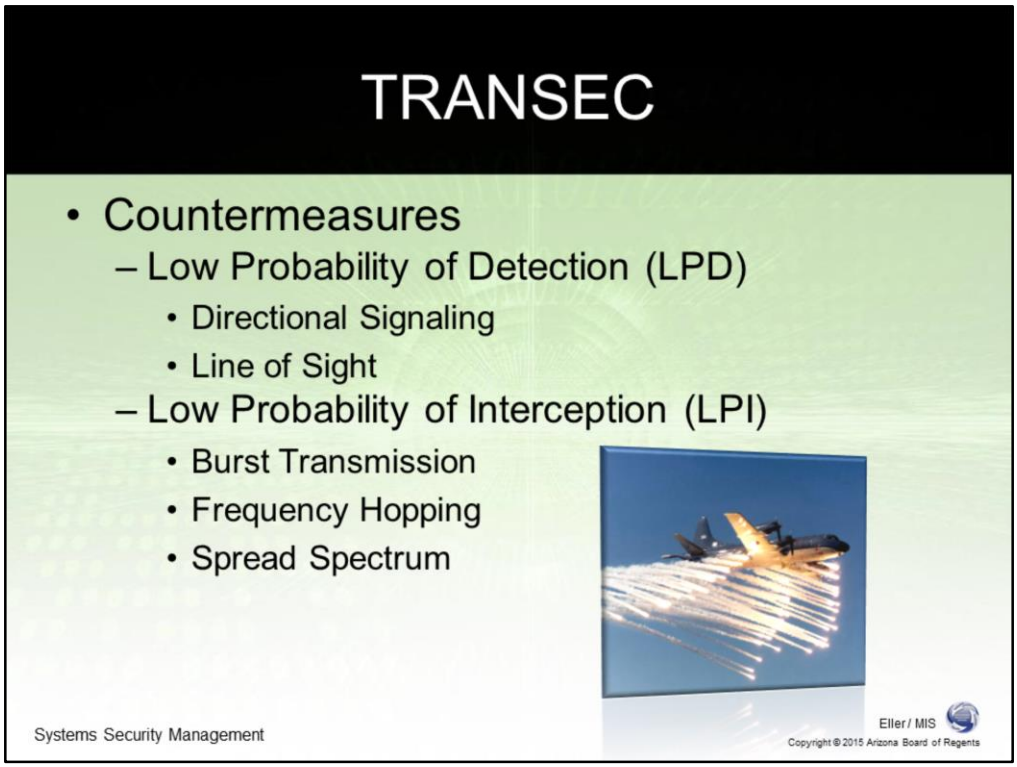
- **RF Fingerprinting** – This vulnerability involves identifying the radio frequency (RF) device based on the frequency behavior of the transmission.
- **Radio Direction Finding (RDF)** – This vulnerability involves triangulating the signal of interest through the use of directional antennas at two or more monitoring stations.
- **Traffic Analysis** – All data transmissions use specific protocols for sending and receiving data, and an attacker can use traffic analysis tools to glean information once the specific protocols being used are identified.
- **Signals Collection** – This vulnerability involves collecting different transmission signals and extracting information from them.



TRANSEC (continued)

Attacks on transmissions can occur through a number of different means. Some of the more common ones include:

- **Eavesdropping** – Eavesdropping is simply finding ways to listen in on voice conversations. This can occur by standing in close proximity to the people having the conversation, using bugs, or finding ways to tap into communication lines.
- **Covert Channels** – A mechanism that while now designed for communication can nonetheless be abused to allow information to be communicated down from a higher compartment of security to one of lower security.
- **Sniffing** – Sniffing takes advantage of the traffic analysis vulnerability. By using specific tools, such as Wireshark or Kismet (for wireless sniffing), an attacker can intercept and monitor network communications in an effort to intercept specific data transmissions.
- **Jamming** – Jamming involves the insertion of noise into a transmission, making it impossible to complete the transmission. This is an active deception technique designed less to intercept the information, but more to make communication more difficult.

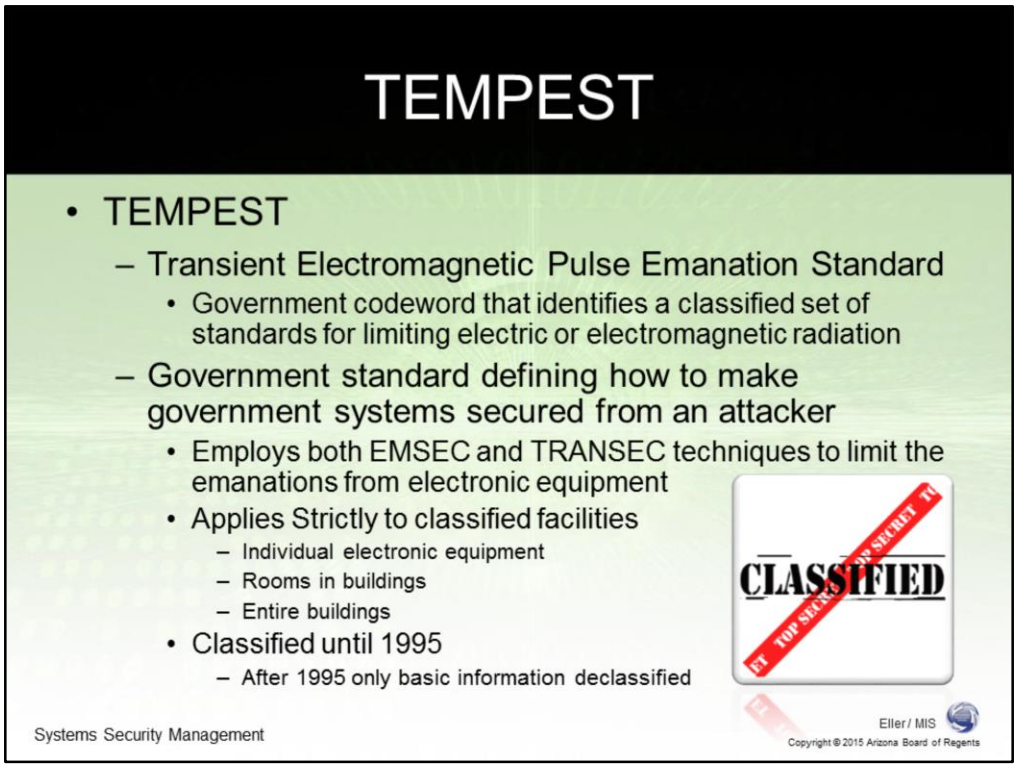


TRANSEC (continued)

There are a number of methods for countering transmission attacks. Some of these methods include:

Low Probability of Detection (LPD) – LPD techniques are used to make it harder for the attacker to detect presence of the signal. Some methods for accomplishing this involve **directional signaling**, sending signals in a specific direction instead of broadcasting in all directions, and **line of sight transmission**, used only for short distance transmissions.

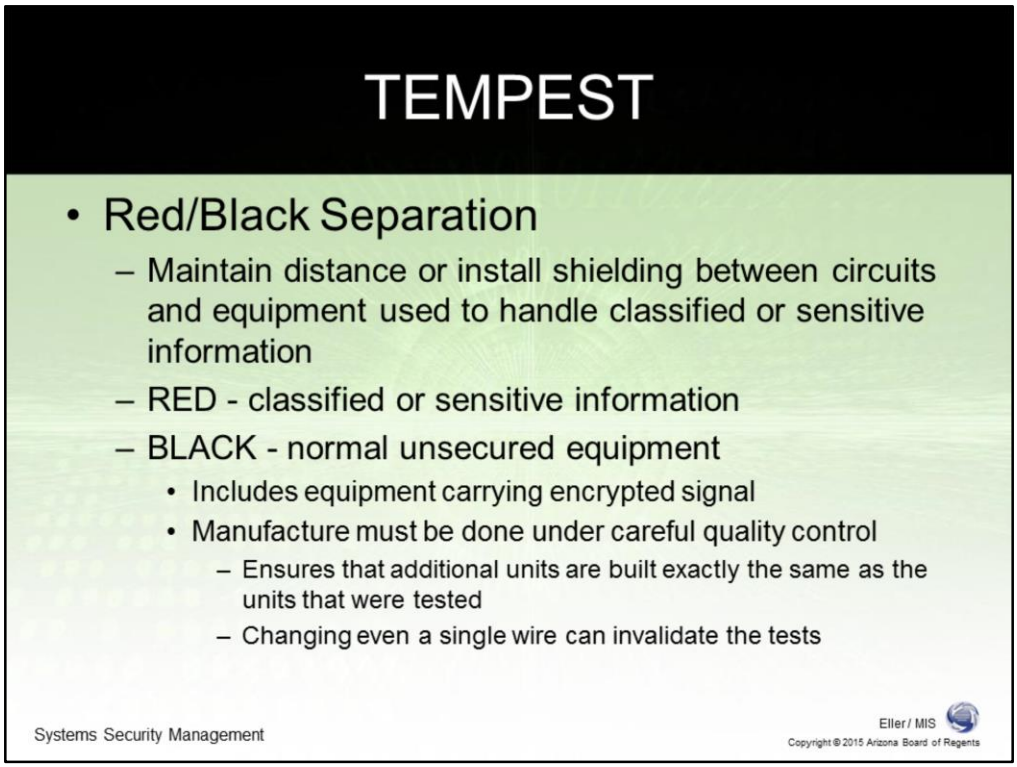
Low Probability of Interception (LPI) – LPI techniques are used to make it harder for attackers to intercept the signals. Some methods for accomplishing this involve **burst transmissions,** sending data in short bursts instead of continuous transmissions, **frequency hopping**, where transmissions hop from one frequency to another frequency with a predefined pseudorandom sequence, and **spread spectrum**, which combines information-bearing sequences with a higher-rate pseudorandom sequence.



TEMPEST

TEMPEST, or the Transient Electromagnetic Pulse Emanation Standard, is a government codeword that identifies a classified set of standards for limiting electric or electromagnetic radiation. As such, it is a government standard defining how to make government systems more secure from an attacker, employing both EMSEC and TRANSEC techniques to limit the emanations from electronic equipment.

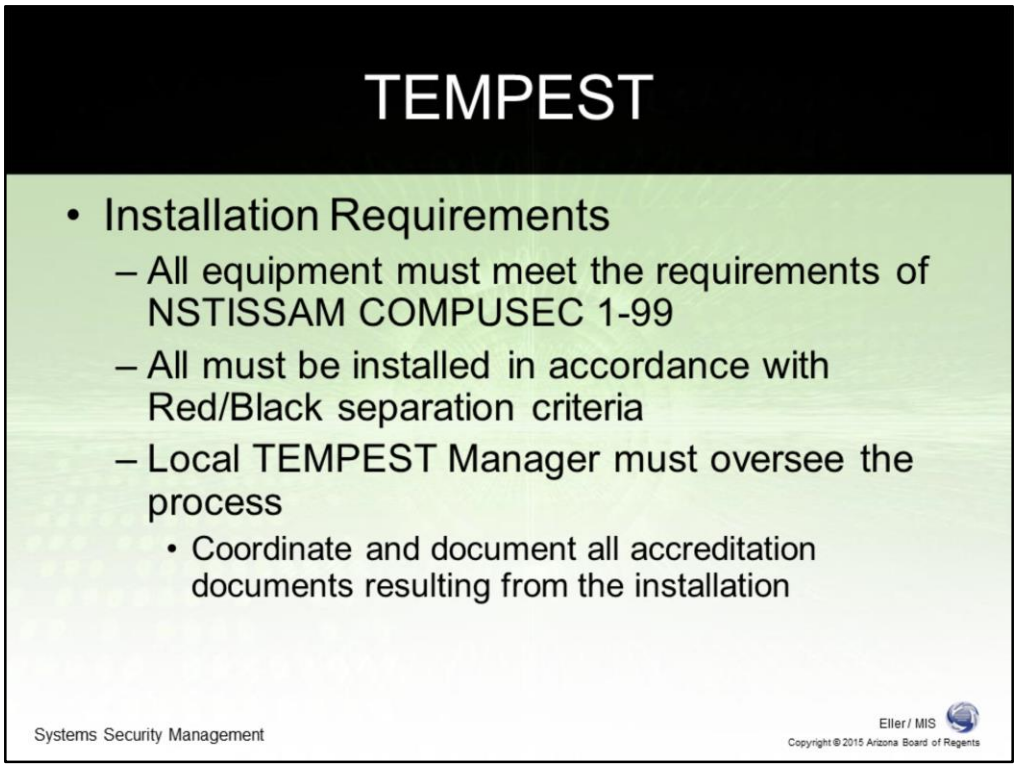
TEMPEST applies strictly to classified facilities housing individual electronic equipment, facilities that have only a few rooms that need to be secured, and even entire buildings if necessary. The TEMPEST program was classified until 1995, at which point only basic information about TEMPEST was declassified.



TEMPEST (continued)

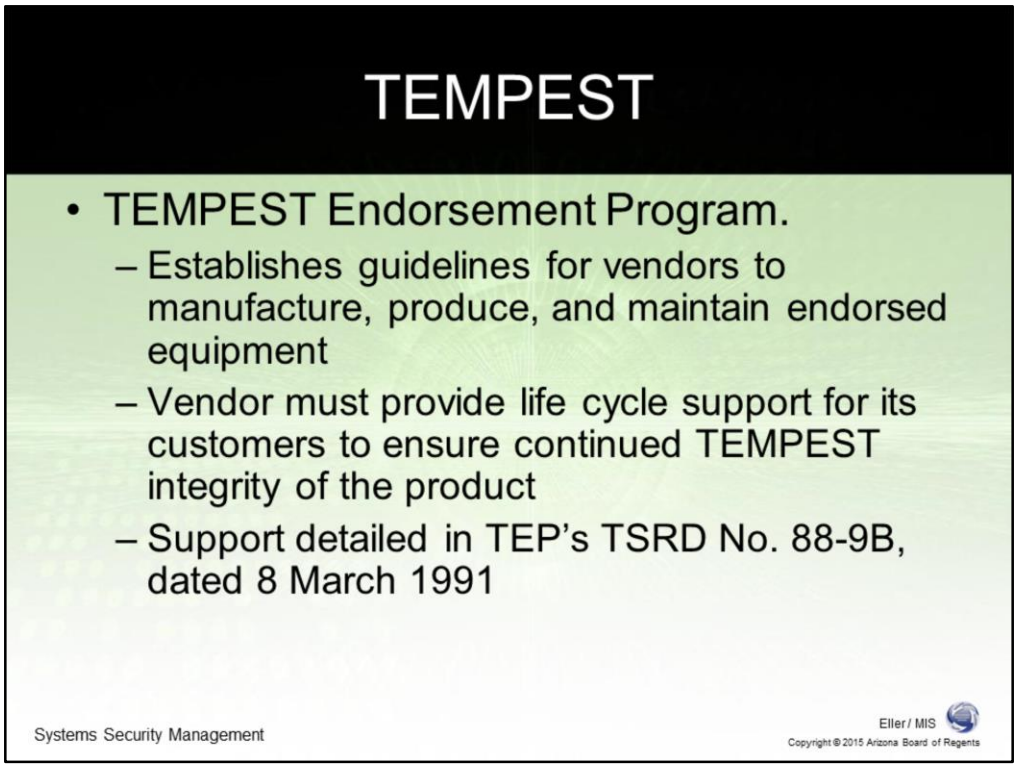
One important aspect of TEMPEST involves the idea of Red/Black separation. This type of separation involves maintaining a distance or installing shielding between circuits and equipment used to handle classified or sensitive information.

In general, Red systems are used to handle classified or sensitive information while Black systems are normal, unsecured equipment. This includes equipment that carries an encrypted signal. Since this involves a tight set of security standards, the manufacture of equipment must be done under careful quality controls to ensure that additional units are built exactly the same as the units that were tested. Changing even a single wire can invalidate the tests.



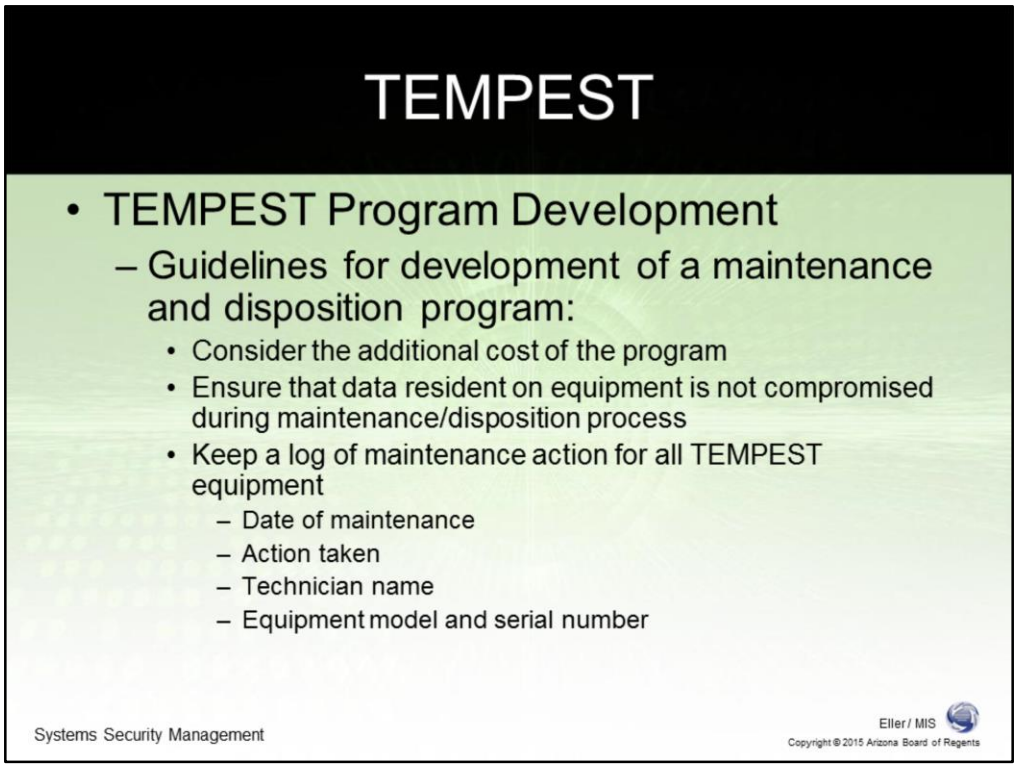
TEMPEST (continued)

TEMPEST equipment must meet a rigid set of installation requirements in order to be approved for use. All equipment must meet the requirements of the National Security Telecommunications and Information Systems Security Association Memorandum COMPUSEC 1-99, which we will discuss later in this lecture. All equipment must be installed in accordance with Red/Black separation criteria. Finally, a local TEMPEST manager must oversee the installation process, coordinating and documenting all accreditation documents resulting from the installation.



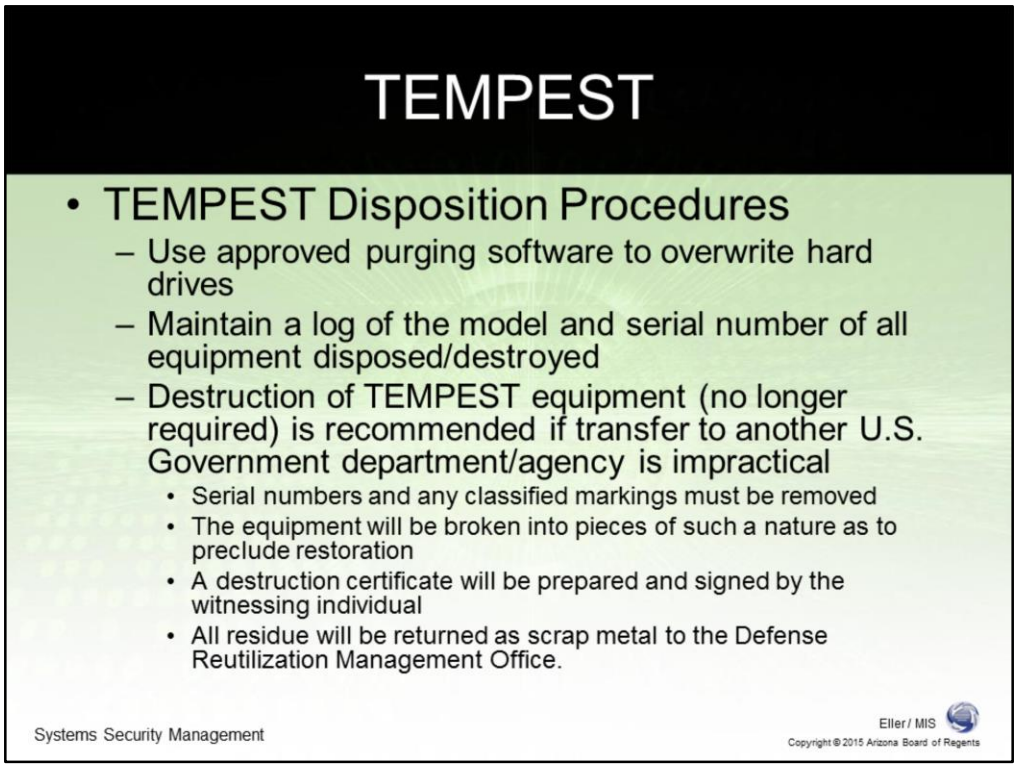
TEMPEST (continued)

The TEMPEST endorsement program was designed to establish guidelines for vendors to manufacture, produce, and maintain endorsed equipment. The vendor must provide life cycle support for its customers to ensure continued TEMPEST integrity of the product. Support of TEMPEST equipment is detailed in the TEMPEST Endorsement Programs's TSRD No. 88-9B, dated 8 March 1991.



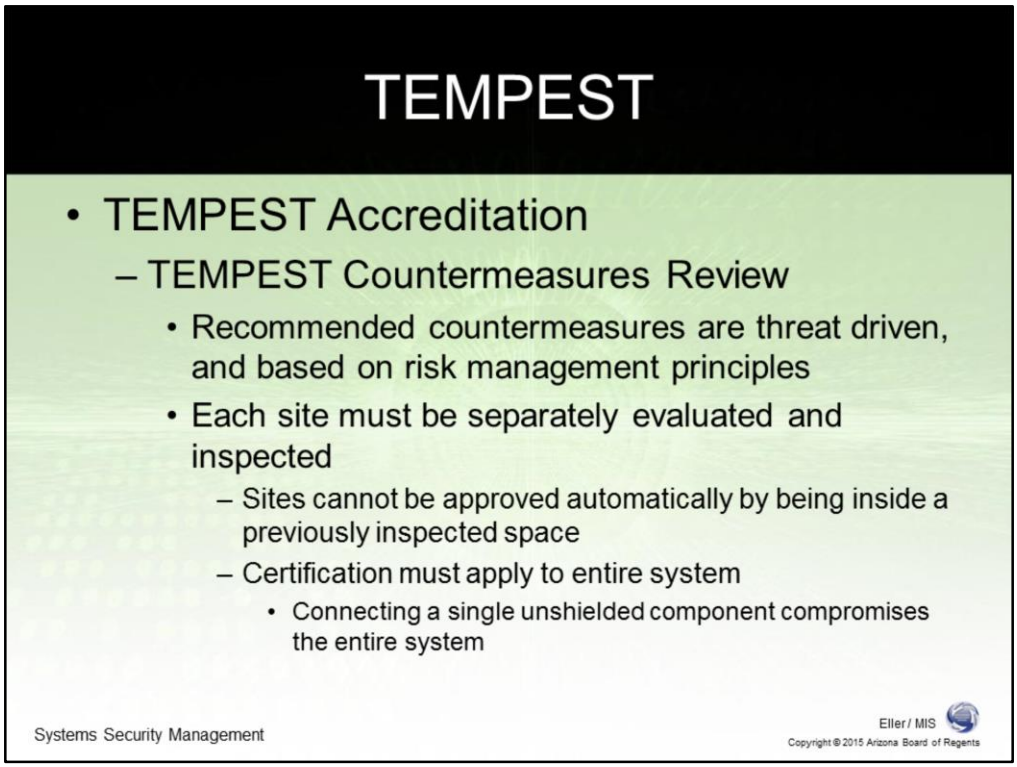
TEMPEST (continued)

In order to develop a TEMPEST program, the government needed to create guidelines for development of a maintenance and disposition program. These guidelines take into consideration the additional cost of implementing a TEMPEST program and ensure that data resident on equipment is not compromised during the maintenance and disposition process. TEMPEST managers are required to keep a log of maintenance action for all TEMPEST equipment including the date of maintenance, the action taken, the technician name, and the equipment model and serial number.



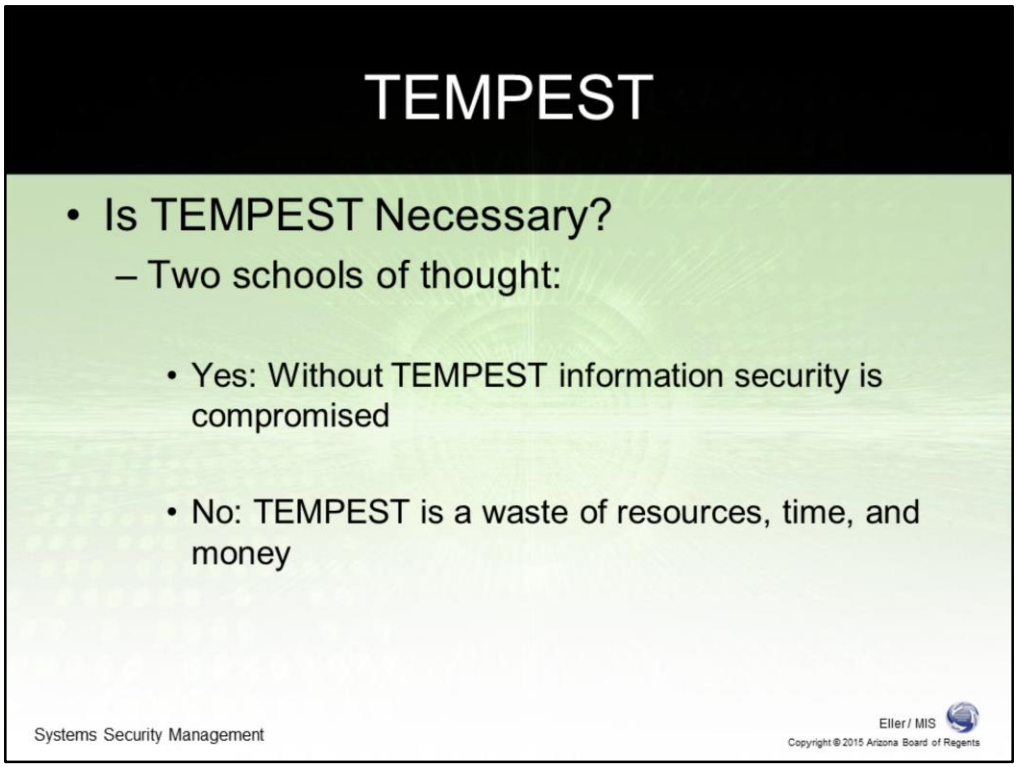
TEMPEST (continued)

TEMPEST disposition procedures involve using approved purging software to overwrite hard drives in order to prevent the loss of sensitive data. A log must be maintained of the model and serial numbers of all equipment that is disposed of or destroyed. While the destruction of TEMPEST equipment is no longer required, it is recommended if the transfer of the equipment to another U.S. Government agency is impractical. If destruction of the equipment is chosen, there are several steps that must be taken. Serial numbers and any classified markings must be removed. The equipment must be broken into so many pieces as to preclude the possibility they could be reassembled into a working system. A destruction certificate will be prepared and signed by an individual who witnesses the destruction. Finally, all residue left over after the destruction will be returned as scrap metal to the Defense Reutilization Management Office.



TEMPEST (continued)

In order for a TEMPEST site to receive accreditation, the site must undergo a countermeasures review. These countermeasures are recommended based on current threats and risk management principles. Each site must be evaluated separately and inspected in order to ensure all TEMPEST requirements are met, and sites cannot be approved automatically solely because they are already inside a previously inspected space. TEMPEST certification will apply to the entire system at the site, since connecting a single unshielded component will compromise the entire system.



TEMPEST (continued)

So now that you have been presented with all of this general information about the TEMPEST program, is TEMPEST really necessary? There are two schools of thought on the subject: yes and no.

The Yes side believes that without TEMPEST then information security is already compromised.

The No side believes that TEMPEST is a waste of resources, time, and money.

TEMPEST (continued)

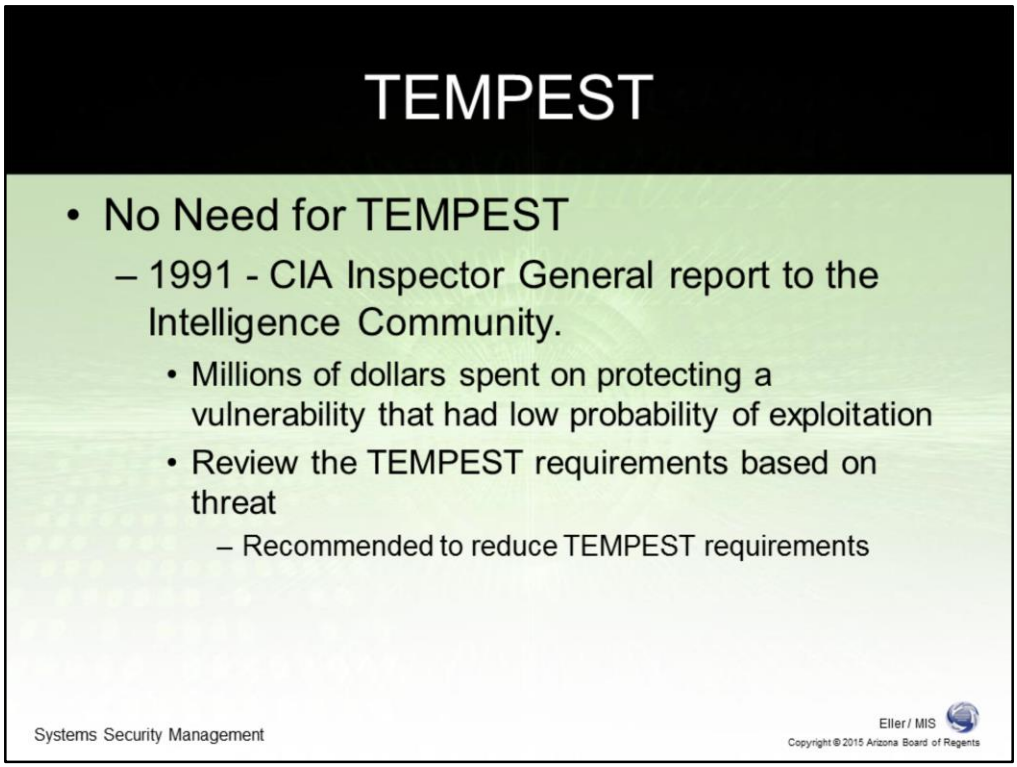
In 1994, the Joint Secretary Commission report to the Secretary of Defense and Director of Central Intelligence made the following statement in support for the TEMPEST program:

"The fact that electronic equipment gives off electromagnetic emanations has long been a concern of the US Government. An attacker using off-the-shelf equipment can monitor and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring."

TEMPEST (continued)

Compromising emanations are a topic covered in a Navy manual. This wording is also used to support the need for a TEMPEST program:

"Foreign governments continually engage in attacks against U.S. secure communications and information processing facilities for the sole purpose of exploring compromising emanations."



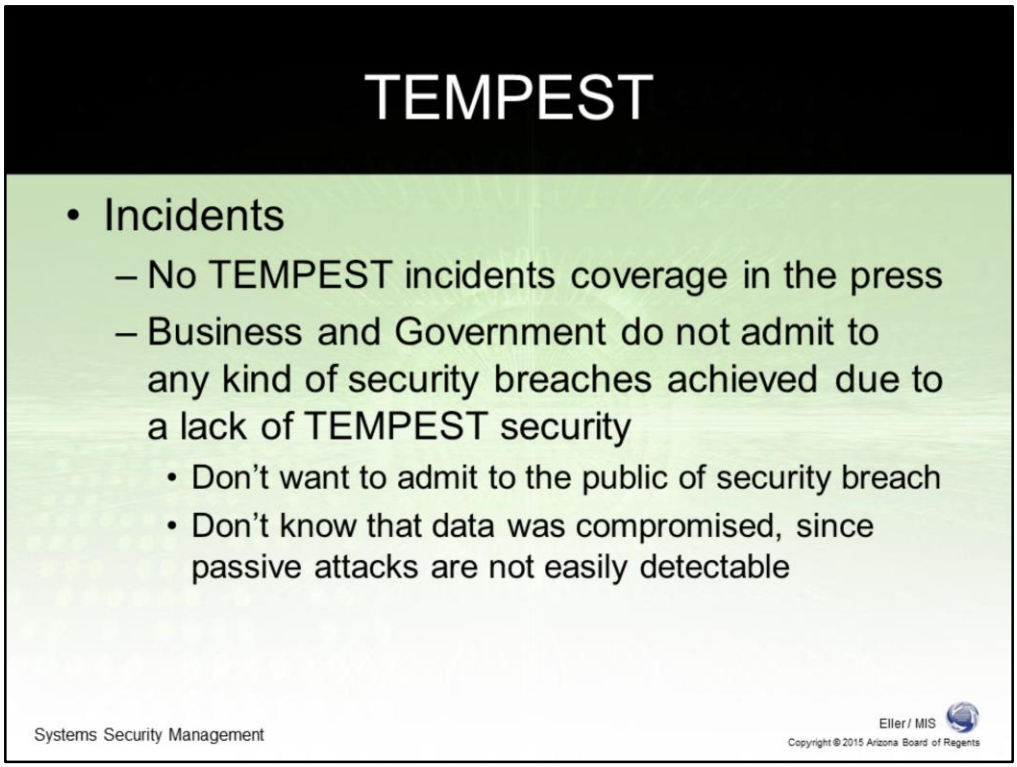
TEMPEST (continued)

On the other side of the coin, in 1991, the CIA Inspector General report to the Intelligence Community condemned the TEMPEST program as unnecessary stating that millions of dollars were spent on protecting a vulnerability that had a low probability of exploitation. The report recommended a review of the TEMPEST program requirements based on specific threats and to reduce the requirements.

TEMPEST (continued)

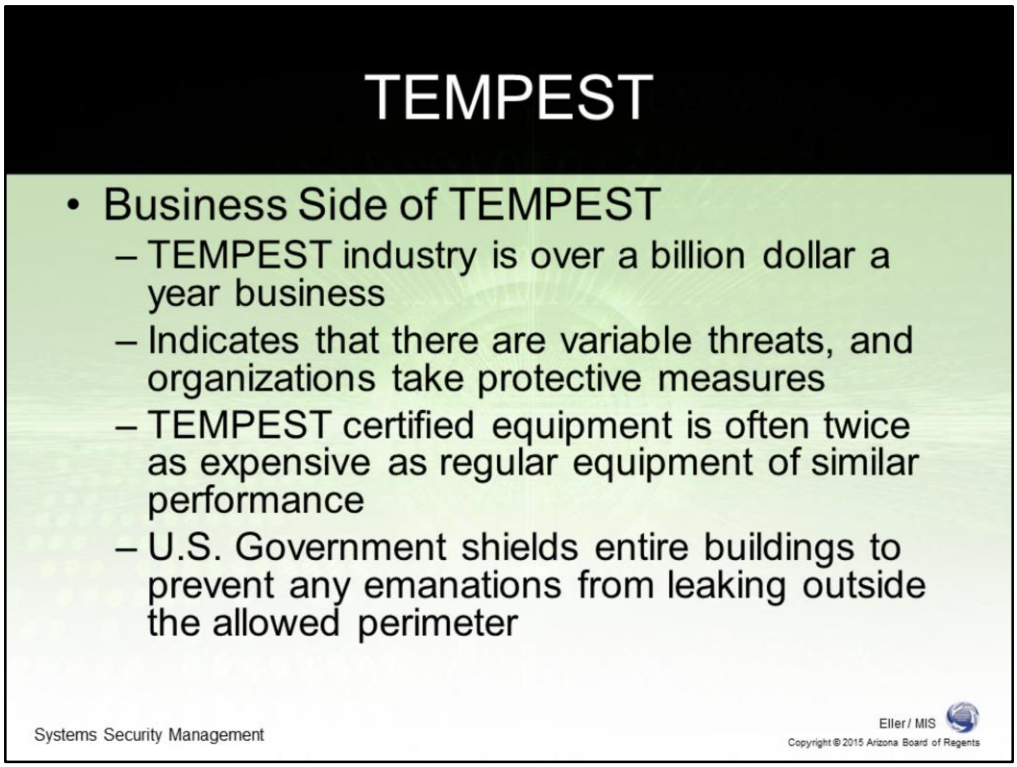
There are a few publicly known examples of why the Government feels there is a need for the TEMPEST program. Some of these examples include the following:

- British MI5 monitoring French traffic noticed enciphered traffic carried a faint secondary signal.
- Replica of Great Seal of the United States presented to U.S. ambassador in Moscow in 1946. In 1952 a problem discovered with the gift as it had listening devices implanted within.
- A new U.S. embassy in Moscow had to be abandoned after large numbers of microphones were found in the structure.



TEMPEST (continued)

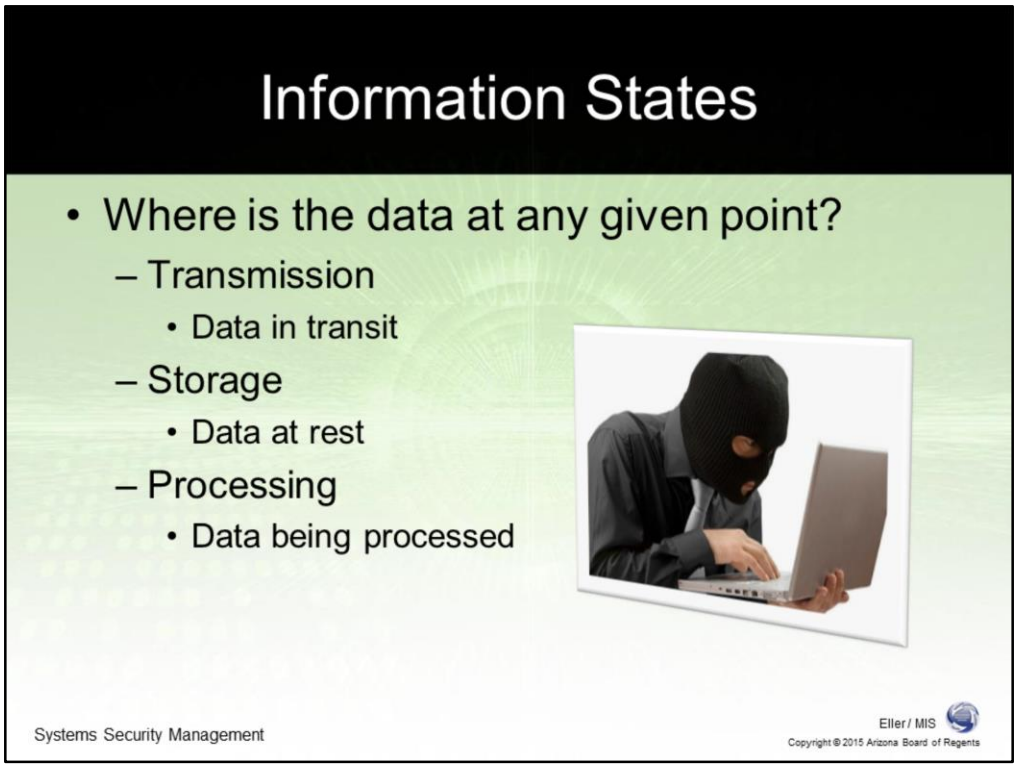
In general there are very few TEMPEST incidents to report of. This is because there is no coverage of TEMPEST incidents in the press. In addition, businesses and Governments do not admit to any kind of security breaches achieved due to a lack of TEMPEST security. This is because they do not want to admit to the public a security breach has occurred, and in many cases they do not know that data was compromised in any way since passive attacks are not easily detectable.



TEMPEST (continued)

Some information on the business side of TEMPEST:

- TEMPEST industry is over a billion dollar a year business
- Indicates that there are variable threats, and organizations take protective measures
- TEMPEST certified equipment is often twice as expensive as regular equipment of similar performance
- U.S. Government shields entire buildings to prevent any emanations from leaking outside the allowed perimeter



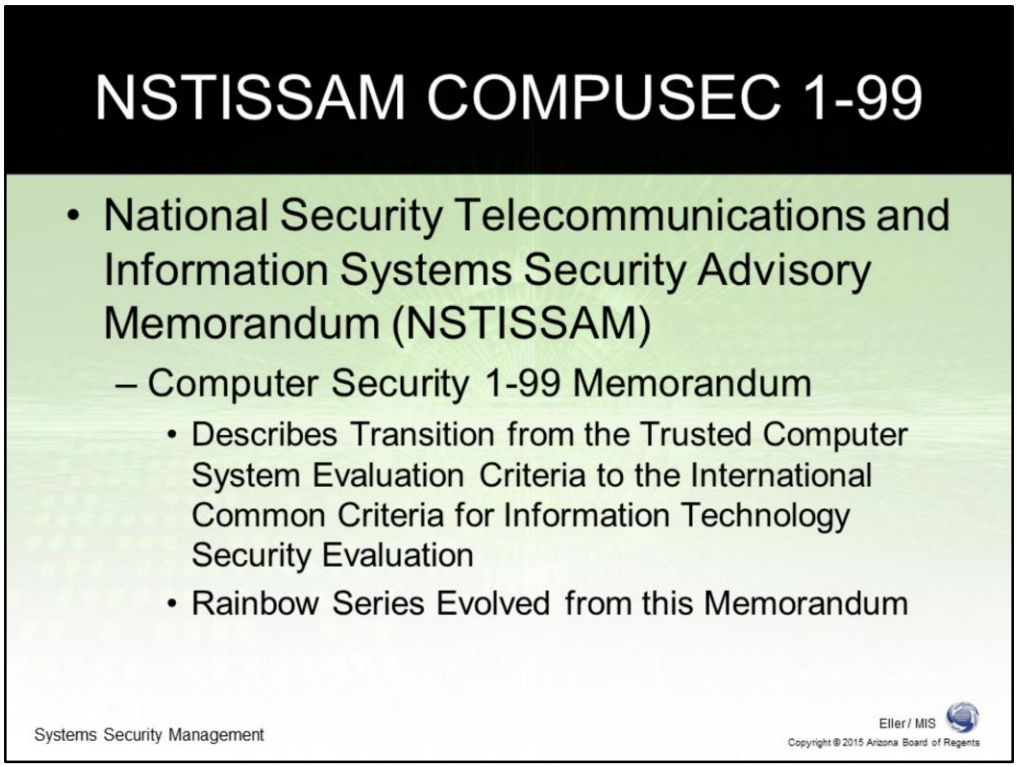
Information States

One of the most important pieces of information assurance comes from an understanding of information states. Where is your data at any given point? There are three main states for information to exist in: transmission, storage, and processing.

Transmission – Transmission occurs when a user has requested data from an information system and when the user saves any compiled information back to the information system. The transmission state needs to be secured because this is when the information is most vulnerable to attack.

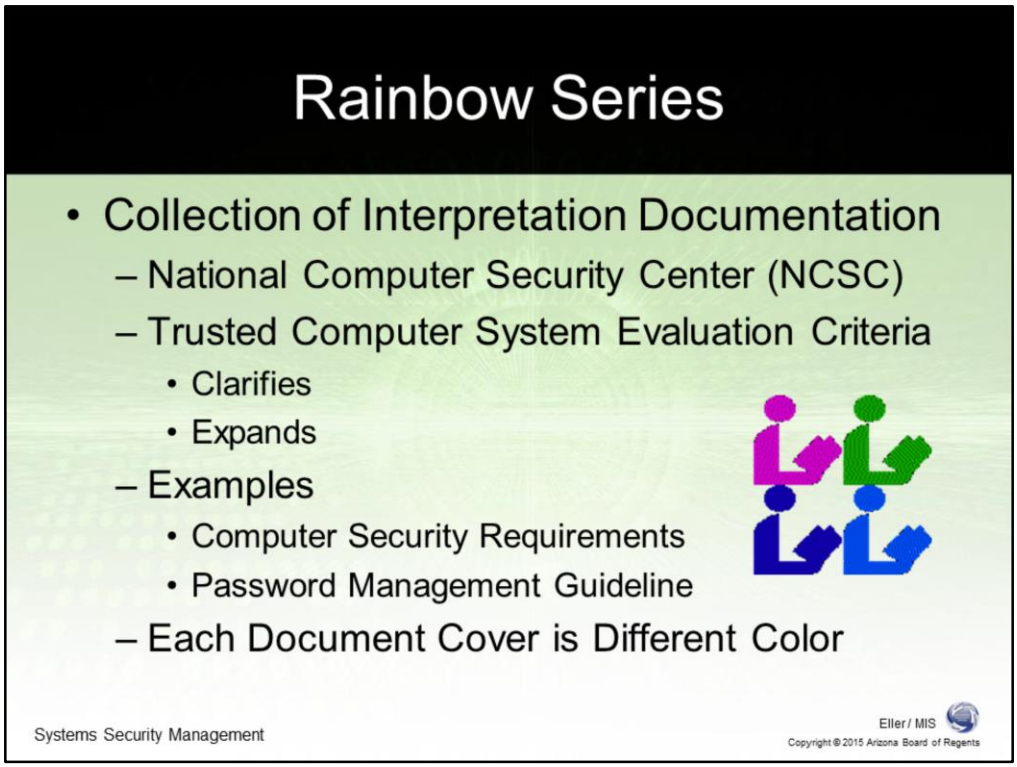
Storage – When data is not being used in any way, the data is stored on information systems. While the data is waiting to be accessed, it can be compromised if the information system is breached. However, information systems are not limited to servers and enterprise storage, there have been lots of reports where breaches occurred because an employee lost an unencrypted laptop or tablet with customer/client information on it. It's important to remember that data can be at rest on any device that can access it, so precautions like whole device encryption or sandbox environments need to be taken to ensure that data is not compromised.

Processing – After retrieving data from an information system, the data will need to be processed into useful information. During the processing state, the data is usually secure; however, this may not be the case if the system processing the data has already been compromised.



NSTISSAM COMPUSEC 1-99

The National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) for Computer Security 1-99 describes the transition from the Trusted Computer System Evaluation Criteria (TCSEC) to the International Common Criteria for Information Technology Security Evaluation. The Common Criteria will be discussed further in Module 5. The Rainbow Series of documents were developed from this memorandum.



The Rainbow Series

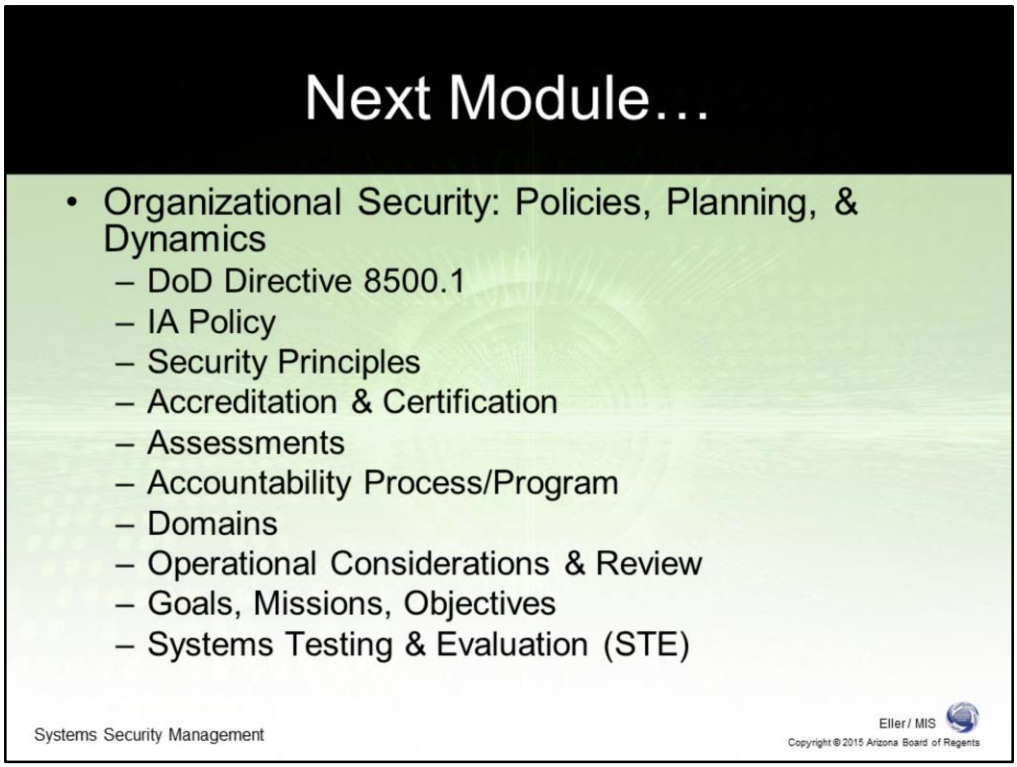
The Rainbow Series is a collection of interpretation documentation developed by the National Computer Security Center (or NCSC). The documentation is a series of trusted computer system evaluation criteria for information assurance. The documents are designed to clarify each topic and expand upon security guidelines as they relate to the Trusted Computer System Evaluation Criteria (or TCSEC). Some examples of Rainbow Series documentation include Computer Security Requirements and Password Management Guidelines. Each document is a different color, which is where the series gets its name. The Rainbow Series documents are available online at the following sites: http://en.wikipedia.org/wiki/Rainbow_Series and http://fas.org/irp/nsa/rainbow.htm.

COMSEC Manager, Policies, and Procedures

A Communications Security Manager is generally a position with a U.S. Government Agency or a Defense Contractor. Someone in this position should have some information security expertise, have experience with business management and is able to deal with people.

COMSEC policies are generally created through government legislation and specific requirements for information assurance programs.

COMSEC procedures have been developed in order to ensure the COMSEC Manager and the COMSEC policies that have been created are accomplishing positive results.



In the next module, we will discuss organizational security as it relates to policies, planning, and dynamics. This will include:

- DoD Directive 8500.1
- IA Policy
- Security Principles
- Accreditation & Certification
- Assessments
- Accountability Process/Program
- Domains
- Operational Considerations & Review
- Goals, Missions, Objectives
- Systems Testing & Evaluation (ST&E)

References

Comsec Manager Competencies. (2008, November 15). *Cabinet Office*. Retrieved from http://www.cabinetoffice.gov.uk/infosec/itpc_certificate_paths/comsec_manager.aspx.

Defense in Depth. (2009). *National Security Agency*. Retrieved from http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

Huggins, D. (2007, July 16). EMSEC in a nutshell. *Spangdahlem Air Base – U.S. Air Force*. Retrieved from http://www.spangdahlem.af.mil/news/story.asp?id=123060796.

Kizza, J. M. (2010). Bare Naked: Emanation, Transmission and Theft of Information. *Computer Science and Electrical Engineering, UT-Chattanooga*. Retrieved from http://www.slidefinder.net/b/bare_naked_emanation_transmission_theft/7441074.

Los, R. (2012, March 29). The information security OODA loop: An introduction. *Infosec Island*. Retrieved from http://www.infosecisland.com/blogview/20783-The-Information-Security-OODA-Loop-An-Introduction.html.

Maconachy, W. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001). A model for Information Assurance: An integrated approach. *Workshop on Information Assurance and Security – U.S. West Point Military Academy*. Retrieved from http://grothoff.org/chrstian/teaching/2007/3704/w2c3.pdf.

Mancini, M. (2014, February 20). Did the Pentagon really ban Furbys? *Mental_floss*. Retrieved from http://mentalfloss.com/article/55136/did-pentagon-really-ban-furbys.

Minihan, K. A. (1999, March 11). Advisory memorandum on the transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation. NSTISSAM/COMPUSEC 1-99. *National Security Telecommunications and Information Systems Security Committee*. Retrieved from http://www.cnss.gov/Assets/pdf/nstissam_compusec_1-99.pdf.

National Security Agency. (2009). NSTISSP No. 11 Fact Sheet. *Committee on National Security Systems*. Retrieved from http://www.niap-ccevs.org/nstissp_11_revised_factsheet.pdf.

Payne, S. C. (2006, June 19). A guide to security metrics. *The SANS Institute*. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/a_guide_to_security_metrics_55.

Trusted Product Evaluation Program. (2009). What is the Rainbow Series? *Stason.org*. Retrieved from http://stason.org/TULARC/security/evaluations/18-What-is-the-Rainbow-Series-Computer-Security-Evaluatio.html.

Usher, A. (2003). Towards a taxonomy of Information Assurance. Retrieved from http://www.sharp-ideas.net/ia/information_assurance.htm.

Zak, A. (2005, March 30). TRANSSEC/EMSEC/TEMPEST. *Polytechnic Institute of New York University*. Retrieved from http://isis.poly.edu/courses/cs996-management-s2005/Lectures/EMSEC-TEMPEST.ppt.