ORS
Office of Radiological Security
Protect · Remove · Reduce

ORS
Office of Radiological Security
Protect · Remove · Reduce

Office of Radiological Security

Cyber Security Program Overview

January 2018

Greg Herdes, CPP, PMP, CISSP
Apogee Group, LLC
Senior Project Manager

NNSA
National Nuclear Security Administration

Global Material Security

ORS
Office of Radiological Security
Protect · Remove · Reduce

Office of Radiological Security

MISSION: The Office of Radiological Security enhances global security by preventing high activity radioactive materials from use in acts of terrorism.

PROTECT

PROTECT radioactive sources used for vital medical, research, and commercial purposes

REMOVE

REMOVE and dispose of disused radioactive sources

REDUCE

REDUCE the global reliance on radioactive sources by promoting the adoption and development of non-radioisotopic alternative technologies

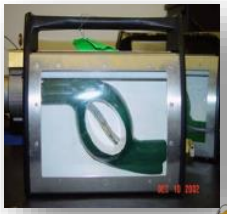
National Nuclear Security Administration
Global Material Security

High Activity Sources

Radionuclide	Normal Device Activity (Ci)
^{60}Co	1,000 – 1,000,000+
^{241}Am	8 – 20
^{192}Ir	10 - 100
^{137}Cs	1,000 – 50,000



Co-60:
Teletherapy and Gamma Knife units (cancer treatment), self-shielded and panoramic irradiators (research and sterilization)




Ir-192:
Radiography (industrial imaging)


Cs-137:
Self-shielded irradiators (research and sterilization), and calibrators (dosimeter and detector calibration)


Am-241:
Oil well logging (industrial imaging)

ORS
Office of Radiological Security
Protect · Remove · Reduce

Protect: Security Enhancements

DETECT
Prompt Detection and Reliable Notification

Next Generation Integrated Remote Monitoring System (Sentry RMS): *Fully networked, hardened, and encrypted security monitor*

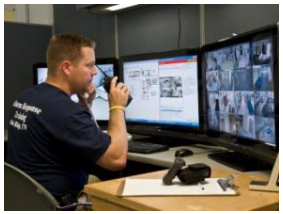
Multi-Factor Access Control: *Requires combination of card, pin, or biometric scan for entry*

DELAY
Extended Adversary Task Time

Hardened Doors

Facility Hardening

RESPOND
Timely, Aware, Equipped and Trained Response



Centralized Monitoring Stations

Personal Radiation Detectors (PRDs) (Domestic only)

TRAIN
Security and Response Training

Alarm Response Training . Response Planning PRD Training, Tabletop Exercises

Security Planning, Performance Testing, Regulatory Development

ORS Containment Strategy

National Nuclear Security Administration

Global Material Security

ORS
Office of Radiological Security
Protect · Remove · Reduce

Cyber and Radiological Security

- Cyber security is one of many critical elements in a comprehensive radiological security program
- Increased emphasis is being placed on cyber security due to recent active targeting of digital systems
- The adversary can take advantage of a spectrum of physical, cyber, and **blended attack** scenarios to achieve high consequence events
- Performing cyber attacks require minimal investment and have minimal chances of attribution or prosecution

Physical Security & Cyber Security Parallels

ORS
Office of Radiological Security
Protect · Remove · Reduce

ASIS INTERNATIONAL™

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

INDUSTRY STANDARDS

Similarities between Physical Security Measures and Cyber Security Controls		
Security Function	Physical Security Measures	Cyber Security Controls
Detection	Intrusion Detection Systems — Motion Sensors — Balanced Magnetic Switches Access Controls Video Surveillance Systems Onsite Security Staff Observation Searches Material inventories Tamper indicating devices	Cyber security staff Network Intrusion Detection Systems Host Intrusion Detection Systems Anti-malware software Security Information and Event Management Systems Critical alert emails and texts Log files Honeypots/Sandboxes/Jails
Delay	Locks Doors Walls Barriers In Device Delay Tie-downs	Cyber security staff Hardware firewalls Software firewalls Demilitarized Zones (DMZs) https://en.wikipedia.org/wiki/DMZ_(computing) Bastion Hosts https://en.wikipedia.org/wiki/Bastion_host Honeypots/Honeynets/Tarpits https://en.wikipedia.org/wiki/Honeypot_(computing); https://en.wikipedia.org/wiki/Tarpit_(networking) Sandboxes https://en.wikipedia.org/wiki/Sandbox_(computer_security) Digital system hardening
Response	Onsite security response Alarm monitoring Law enforcement response Investigations	Cyber security staff Alarm monitoring Intrusion Prevention Systems Forensic investigations Cyber Security Incident Response

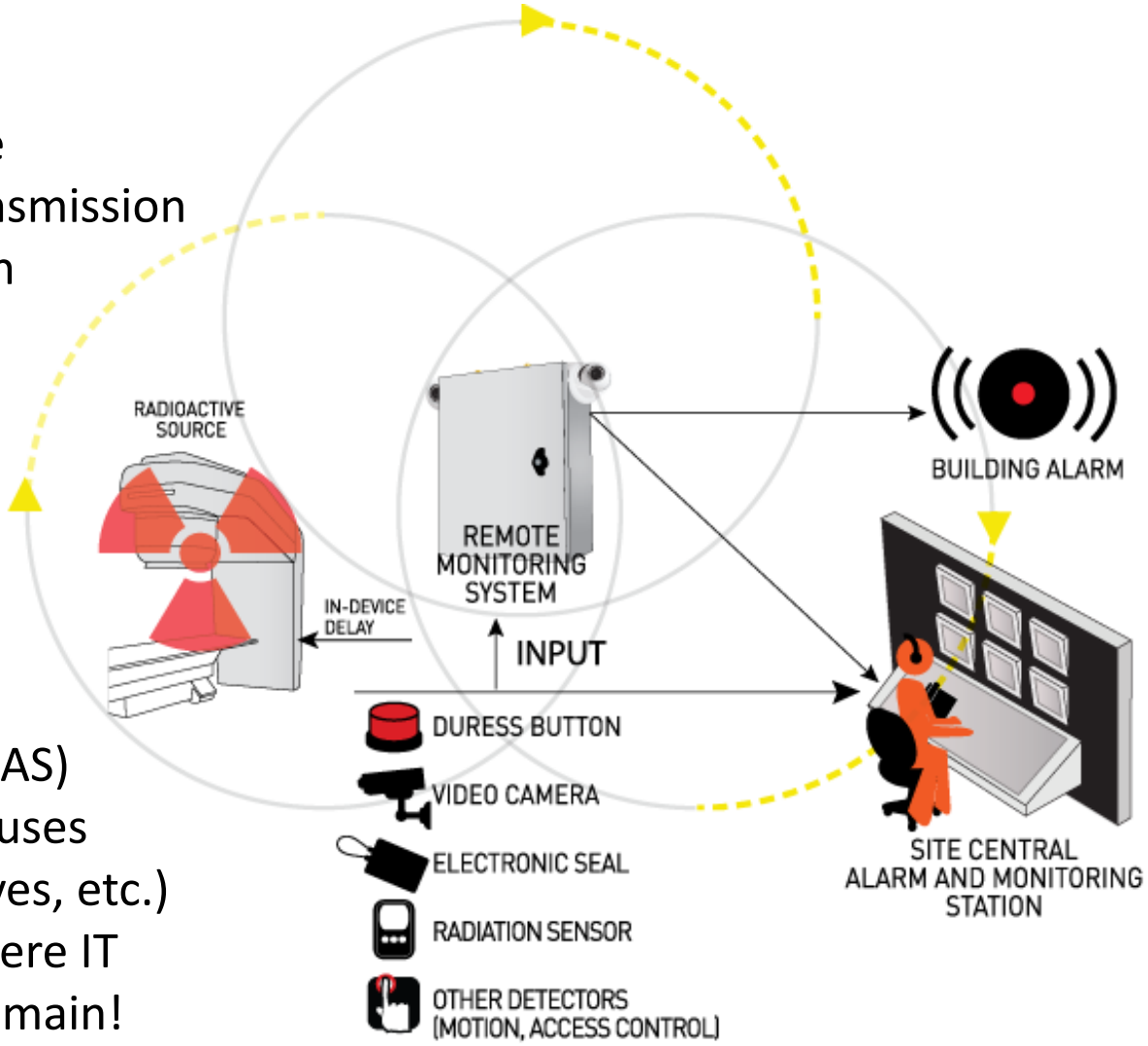
Evolution of Security Systems

- The blending of physical protection systems with information technology is advancing at such a rapid pace that the two can no longer be viewed independently or separately
- Security systems are evolving from stand-alone hardwired devices to network-based devices where both power and data may be provided by a single Ethernet cable
- This is the same type of evolution of phone systems moving from landline copper wires to Voice over Internet Protocol (VoIP) that is common in many offices today
- Cyber security hygiene measures can address many potential issues

ORS
Office of Radiological Security
Protect · Remove · Reduce

Information Technology

- Technology that enables the processing, storage and transmission of information = Information Technology (IT)
- IT has seeped into all aspects of our lives!
- For ORS this means?
  - Security Cameras
  - Access Controls
  - RMS
  - Central Alarm Station (CAS)
  - IT related to rad source uses (irradiators, gamma knives, etc.)
  - LOTS of other places where IT exists within the ORS domain!

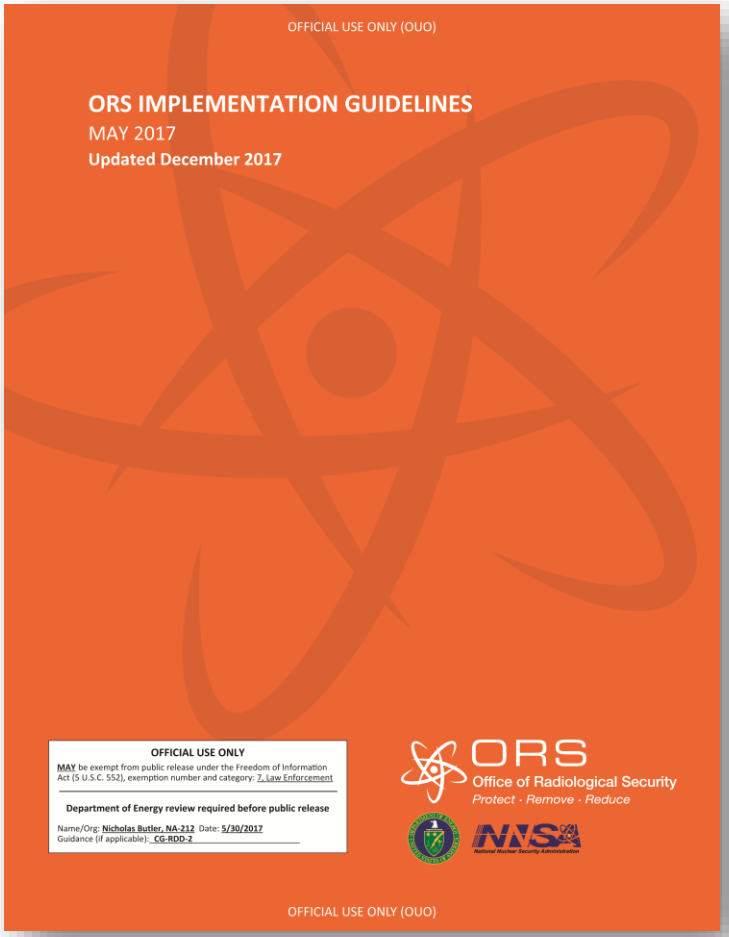


National Nuclear Security Administration

ORS
Office of Radiological Security
Protect · Remove · Reduce

ORS Cyber Security Concerns

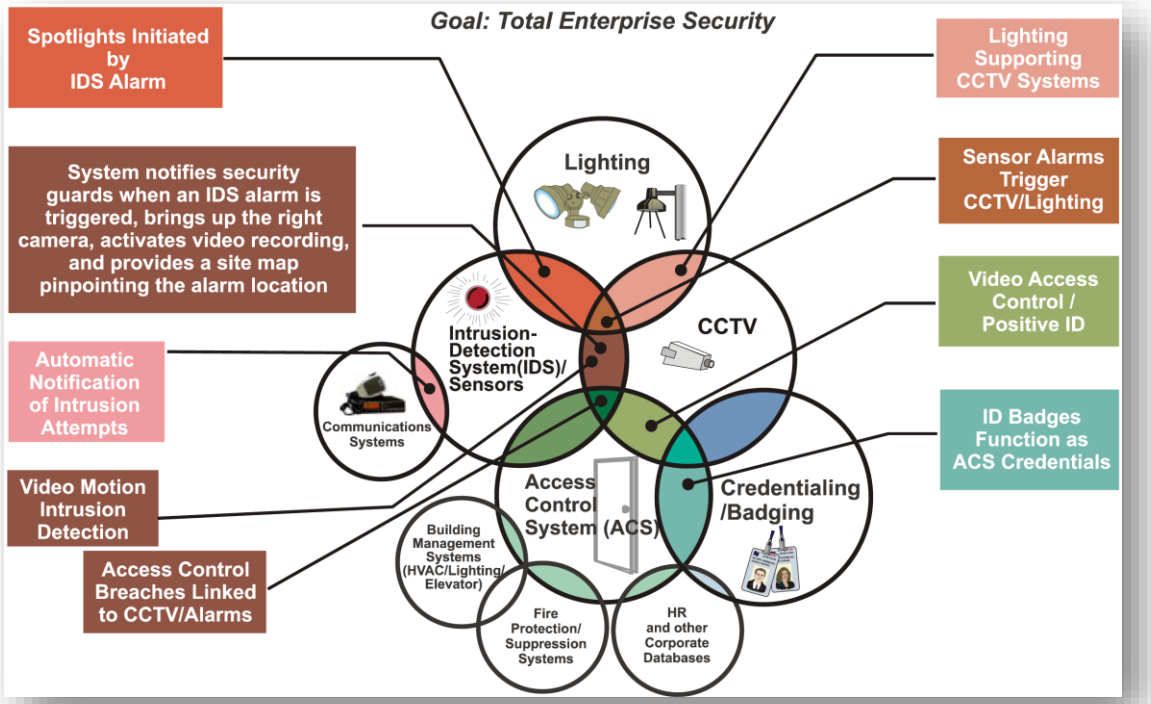
- Adversary using a cyberattack to override a facility's existing network controls and physical security measures, allowing them to facilitate a physical attack
- Adversary exploiting security equipment such as the Sentry RMS to gain access to a site's network(s) to carry out a cyberattack, for example installing ransomware or stealing proprietary or other sensitive information
- Social engineering (e.g., phishing emails or phony web pages) could be used to exploit personnel to gain access to physical security systems, networks, and related subsystems without the need to hack or conduct a cyberattack using cyber tools
- Attack may include site reconnaissance looking for exposed hardware, company information, or written-down passwords



National Nuclear Security Administration
Global Material Security

Security Systems have Cyber Security Issues

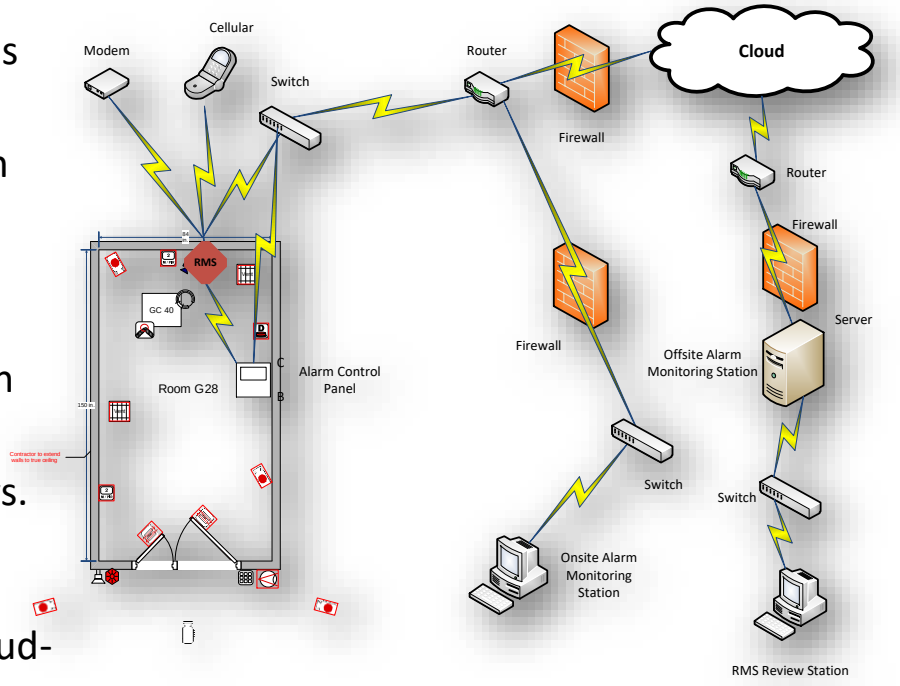
- All security systems contain some form of Intrusion Detection System (IDS), Access Control Systems (ACS), and a method for monitoring alarm states either on-site, off-site, or in many cases both
- The main security system and network related components and capabilities that are potentially vulnerable to cyberattacks include:
  - Alarm concentrators/panels, which communicate to the host over various communication protocols, Ethernet, or combination of protocols.
  - Analog cameras are giving way to IP cameras where Power over Ethernet (PoE) is becoming even more commonplace.
  - Access control systems and enrollment stations



Transit Security Design Considerations, USDOT

Typical ORS Remote Monitoring System and Intrusion Detection System Network Diagram

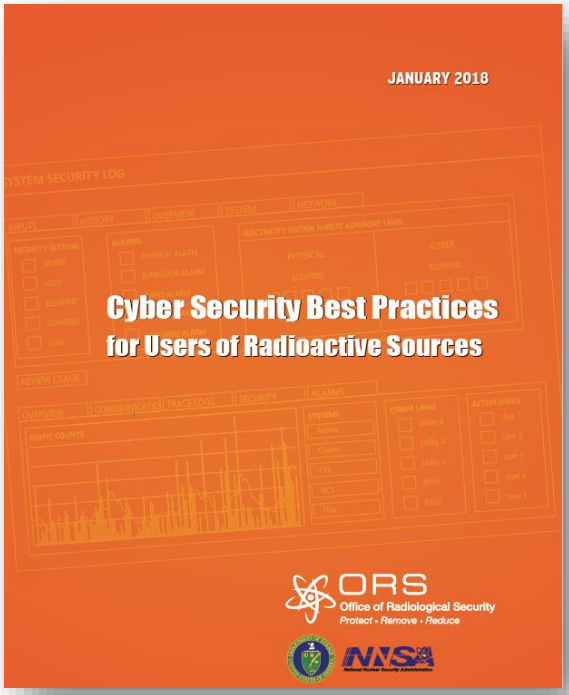
- Network diagram represents a typical domestic middle sized facility such as a small university or hospital
- Demonstrates the potential cyber complexities of a relatively simple one target room facility
- Typical ORS security enhanced irradiator room with the RMS connected to the burglar alarm panel for redundancy
- RMS signals go to an onsite alarm monitoring station and an offsite alarm monitoring station
- There is an endless variety of how networks could be laid out, e.g., firewall before router vs. router before firewall vs. router/firewall combination, network components can be geographically far apart, services could be cloud-based such as IaaS, PaaS, etc.
- Management of facility networks could be outsourced to third parties



ORS
Office of Radiological Security
Protect · Remove · Reduce

ORS Cyber Security Activities

- ORS Cyber Security Best Practices
- Domestic and International Cyber Security Assessments
- Cyber Security Guidance for Installation and Sustainability statements of work
- Cyber security training
- Cyber/Physical Scenarios and Vulnerability Assessments
- Cyber security assessments of ORS-developed equipment
  - Mobile Source Transit Security System (MSTS)
  - Sentry Remote Monitoring System



There is a need to integrate physical and cyber security vulnerability assessments and security programs

NNSA
National Nuclear Security Administration
Global Material Security

ORS
Office of Radiological Security
Protect · Remove · Reduce

CONTACTS

Gregory A. Herdes, CPP, PMP, CISSP
Senior Project Manager
Apogee Group, LLC, Contractor to the
National Nuclear Security Administration
Office of Radiological Security
gregory.herdes@nnsa.doe.gov
+1 (615) 335-5312

Nicholas Butler
Domestic Program Office Director
Office of Radiological Security
National Nuclear Security Administration
nicholas.butler@nnsa.doe.gov
+1 (202) 586-1929

National Nuclear Security Administration
Global Material Security