

Cybersecurity Best Practices for Users of Radioactive Sources

Presented by:
Greg Herdes, CPP, PMP, CISSP
ORS Cybersecurity Lead



September 2019



Global
Material
Security



ORS
Office of Radiological Security
Protect · Remove · Reduce

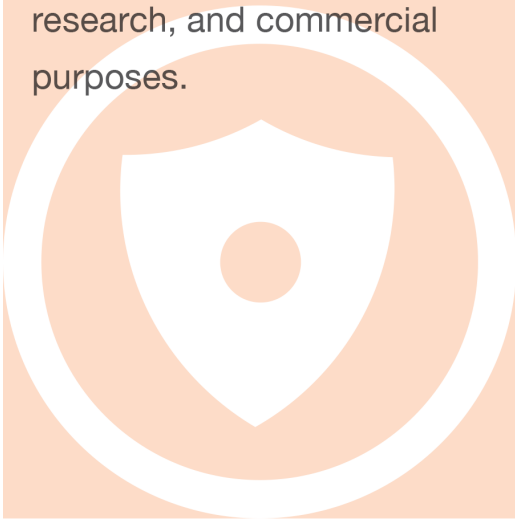
Enhance global security by preventing high-activity radioactive materials from being used in acts of terrorism.



ORS Strategies

PROTECT

Protect radioactive sources used for vital medical, research, and commercial purposes.



REMOVE

Remove and dispose of disused radioactive sources.

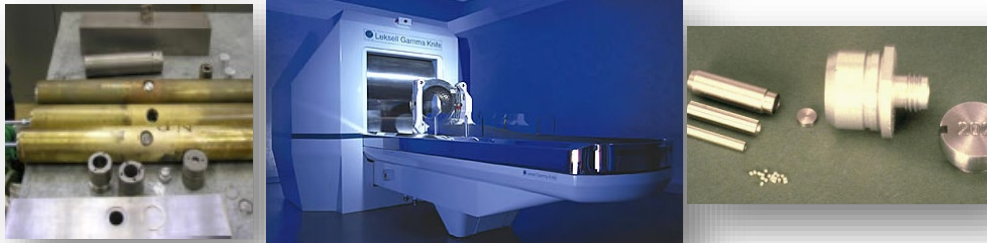


REDUCE

Reduce the global reliance on high-activity radioactive sources by promoting the adoption and development of non-radioisotopic alternative technologies.



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)

Evolution of Security Systems

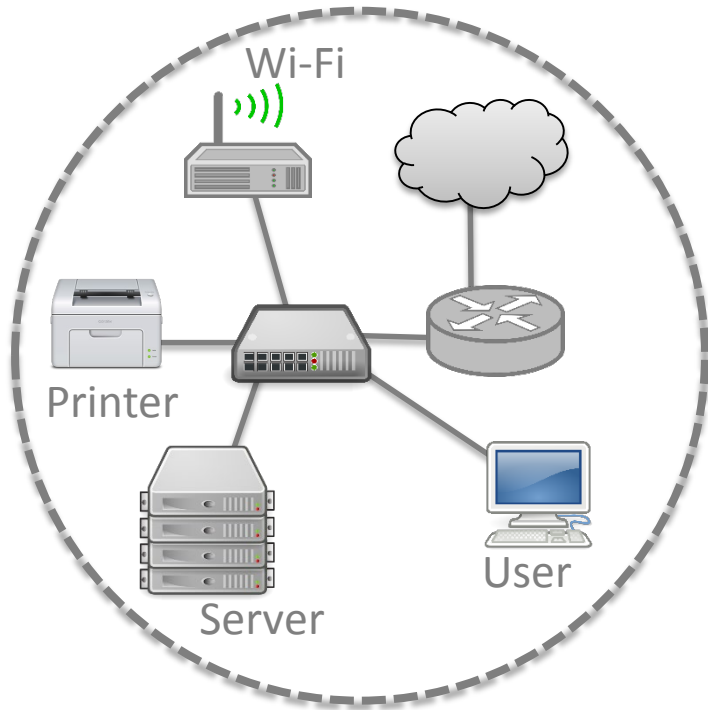
- The blending of physical protection systems with IT is advancing at such a rapid pace that the two can no longer be viewed independently or separately
- Security systems are evolving from stand-alone hardwired devices to network-based devices where both power and data (information) may be provided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




ORS Cybersecurity Concerns

- Adversary using a cyberattack to override a facility's existing network controls and physical security measures, allowing them to facilitate a physical attack – Blended 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, stealing proprietary or other sensitive information, or disrupting operations
- 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

BASIC CYBERSECURITY PRINCIPLES



Security is a process

 Every system has vulnerabilities

Impossible to
eliminate all
of them



SYSTEMS CHANGE OVER TIME

- System requirements change over time
- Systems change over time



SYSTEMS REQUIRE MAINTENANCE

- Check for defunct users
- Update virus software
- Patch security holes
- Test firewalls

GOAL: ASSURANCE

The principle of ALARA, “as low as reasonably achievable”
applies to cybersecurity as well as radiation safety by limiting exposure

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**

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

Physical Security & Cybersecurity

Similarities between Physical Security Measures and Cybersecurity Controls		
Security Function	Physical Security Measures	Cybersecurity Controls
Detection	Intrusion Detection Systems <ul style="list-style-type: none"> - Motion Sensors - Balanced Magnetic Switches Access Controls Video Surveillance Systems Onsite Security Staff Observation Searches Material Inventories Tamper Indicating Devices	Cybersecurity 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	Cybersecurity Staff Hardware Firewalls Software Firewalls Demilitarized Zones Bastion Hosts Honeypots, Honeynets, Tarpits Sandboxes Digital System Hardening
Response	Onsite Security Response Alarm Monitoring Law Enforcement Response Investigations	Cybersecurity Staff Alarm Monitoring Intrusion Prevention Systems Forensic Investigations Cybersecurity Incident Response

Industry Standards



American Society for Industrial Security (ASIS) International

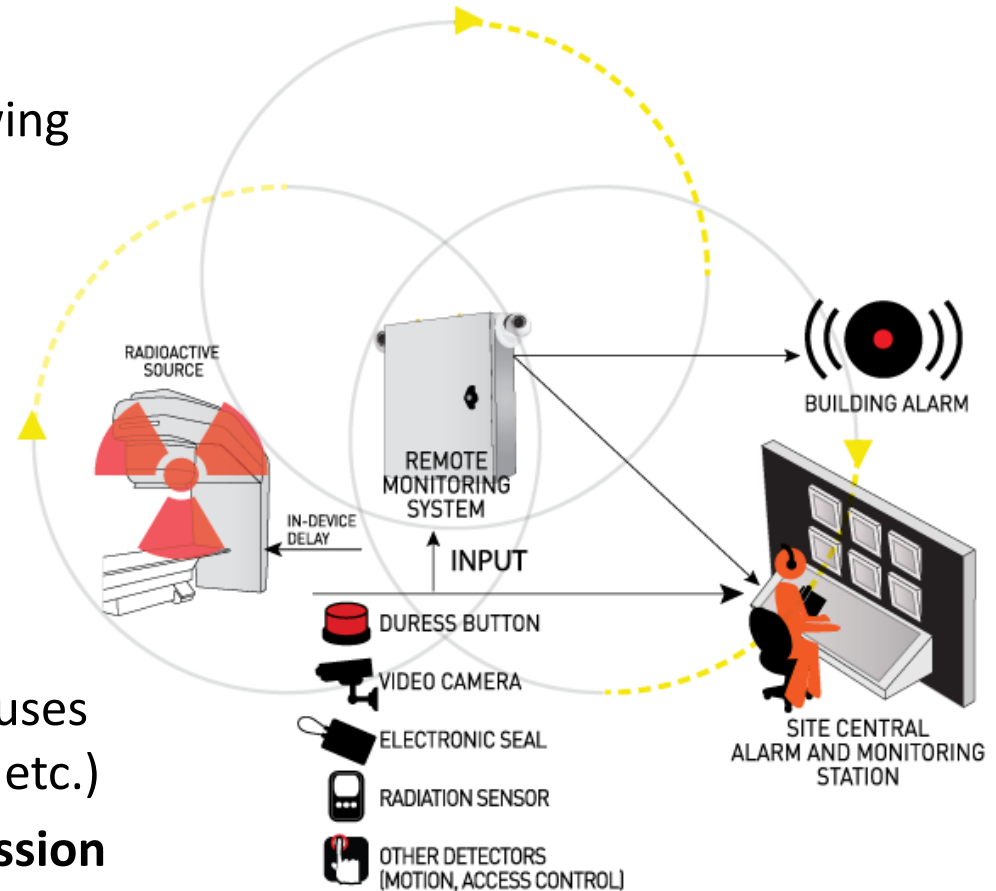


Global Material Security

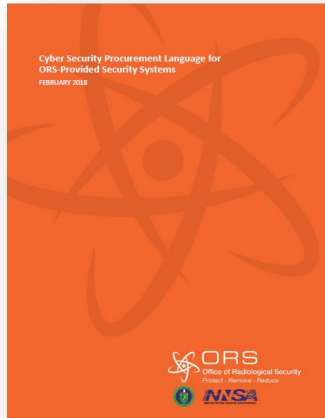


ORIS
Office of Radiological Security
Protect · Remove · Reduce

- For ORS this includes the following equipment and technologies:
 - Security Cameras
 - Access Controls
 - RMS
 - Central Alarm Station (CAS)
 - Personnel records
 - Information Technology (IT) related to radiation source uses (irradiators, gamma knives, etc.)
 - **IT exists within the ORS mission**



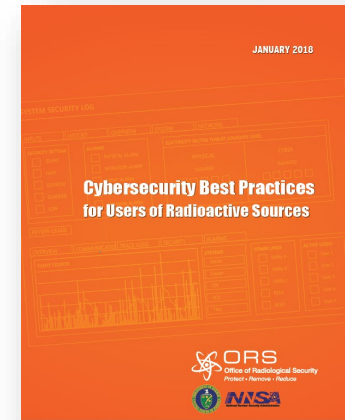
ORS Cybersecurity Tools



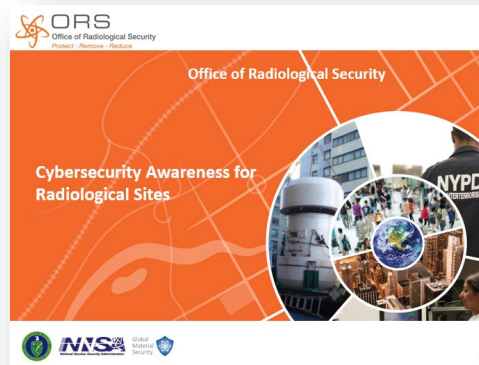
Procurement Requirements



Implementing Guidelines



Best Practices



Training For Regulators, Site Security Officers, and Security Vendors



Training for ORS HQ, Labs, and Physical Protection Staff