National Nuclear Security Administration

Cybersecurity for Gamma Irradiation Facilities

Presented By:

Michael Rowland (Sandia National Laboratories)

Co-Author:

Greg White (LLNL)

November 11, 2022

Global Material Security

ORS Office of Radiological Security

Protect · Remove · Reduce

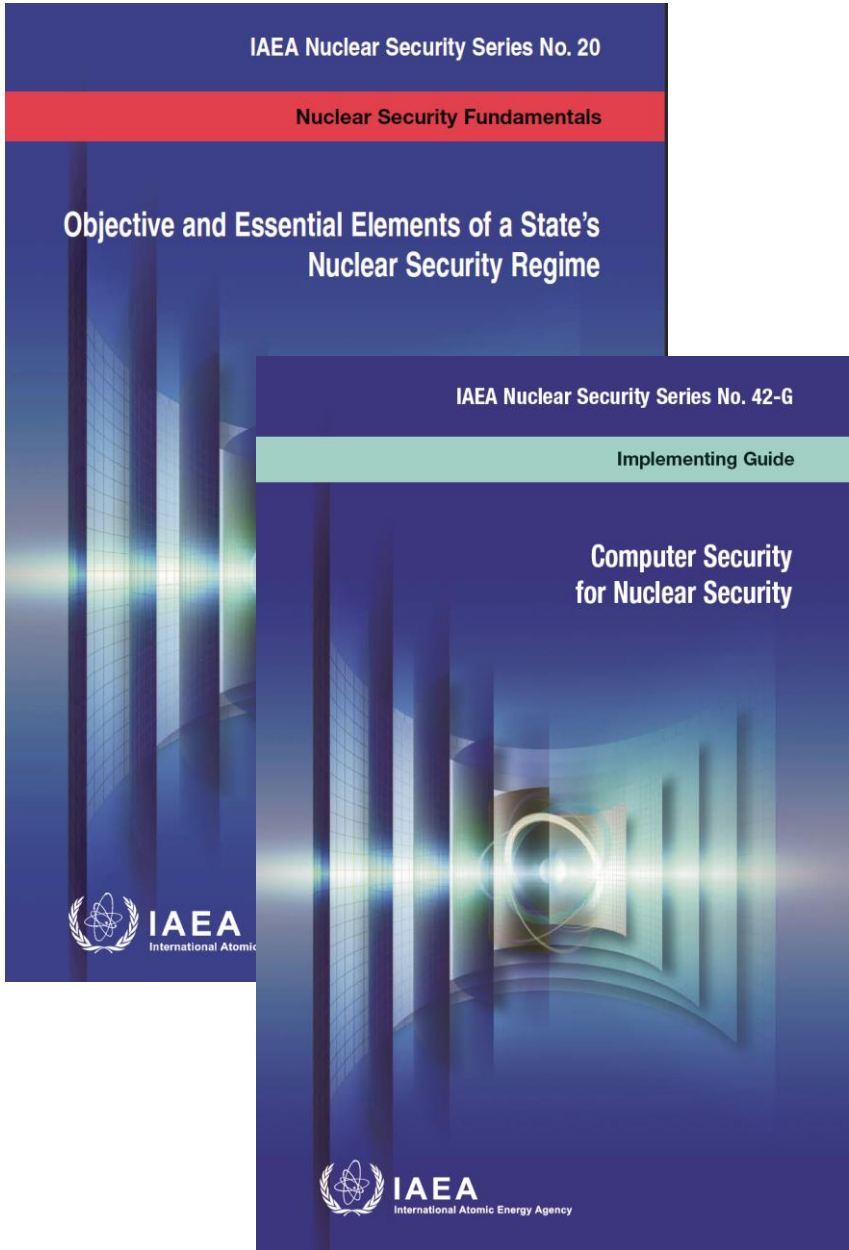
National Nuclear Security Administration

Overview

- IAEA Guidance for Other Radioactive Material and Associated Facilities
- Fundamental Concepts
  - Security Levels
  - Security Zones
  - Defensive Cyber Security Architecture (DCSA)
- Cyber Attack Model
- Threat from Ransomware
- DCSA for Industrial Irradiators
- ORS Guides

Introduction

- IAEA NSS 20 – *Nuclear Security Fundamentals* essential elements to information and computer security are:
  - Information and computer security regulations
  - Secure exchange of sensitive information
  - Graded requirements based on Risk
  - Implementation consistent with defense-in-depth approaches
- IAEA NSS 42-G – *Computer Security for Nuclear Security* provides additional guidance about
  - Graded requirements – computer security levels
  - Defense-in-depth – computer security zones
- NSS 42-G further describes the computer security zones to provide a Defensive Computer Security Architecture (DCSA)



National Nuclear Security Administration

Background

- IAEA NSS 14 – *Nuclear Security Recommendations on Radioactive Material and Associated Facilities* provides additional guidance about
  - Requirements based on defense-in-depth
  - Security requirements based on hardware, procedures and facility design
- NSS 11-G rev 1 – *Security of Radioactive Material in Use and Storage and of Associated Facilities* further applies defense-in-depth to the security functions of
  - Detection
  - Delay
  - Response

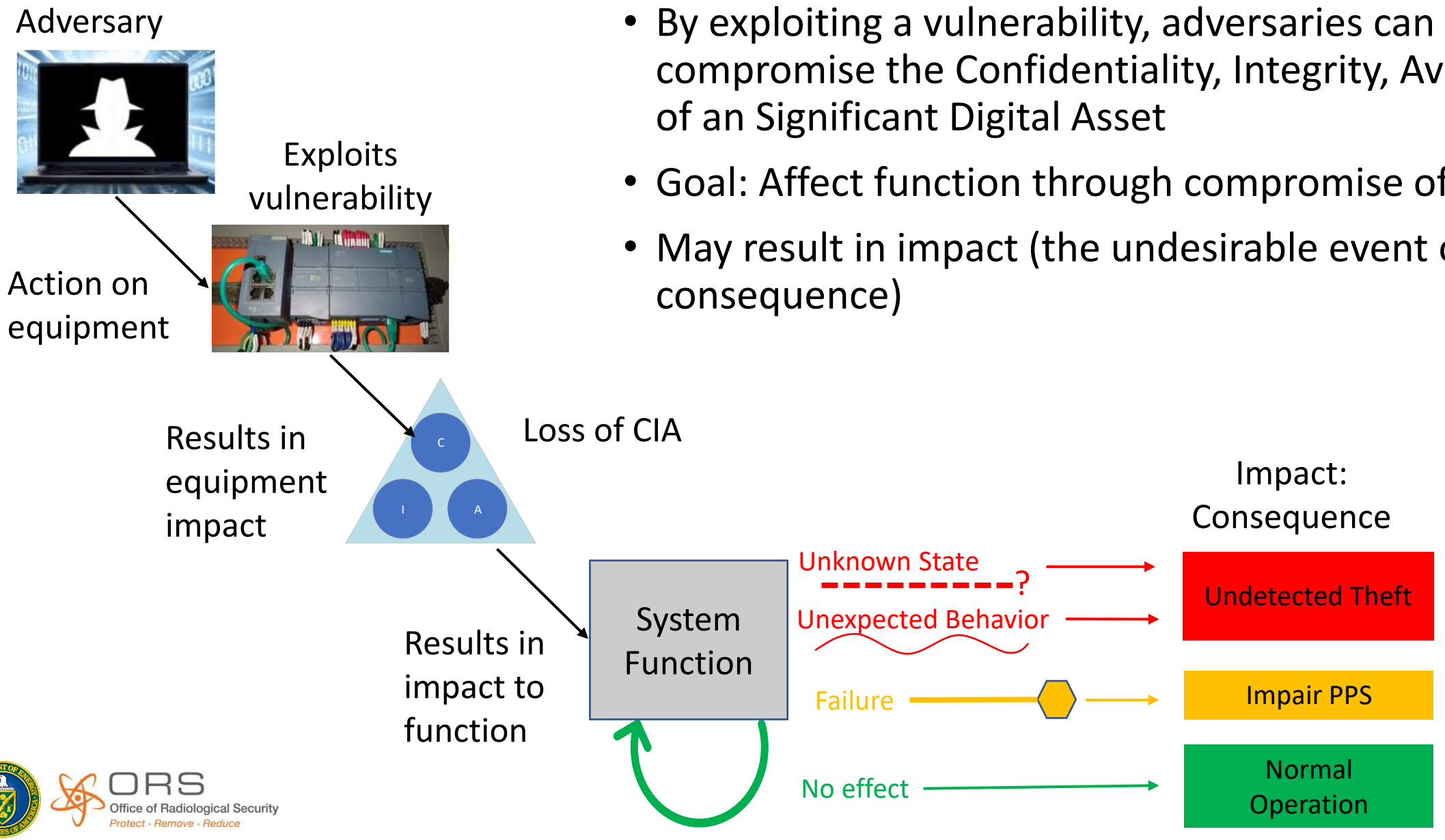
ORS Office of Radiological Security
Protect · Remove · Reduce

Fundamental Concepts

- **Facility Function**: the purpose that needs to be achieved
  - Control of direct physical access to the radioactive source
- **Detection**: detect malicious acts
- **Delay**: delay the progression of a malicious act
- **Response**: respond to a malicious act with sufficient resources to interrupt or prevent the unauthorized removal of radioactive materials
- **Levels**: the strength of security protection for a facility function
- **Zone**: a group of systems having common physical and logical boundaries
  - All zones are assigned to a common security level
- **System**: a set of equipment that perform a facility function

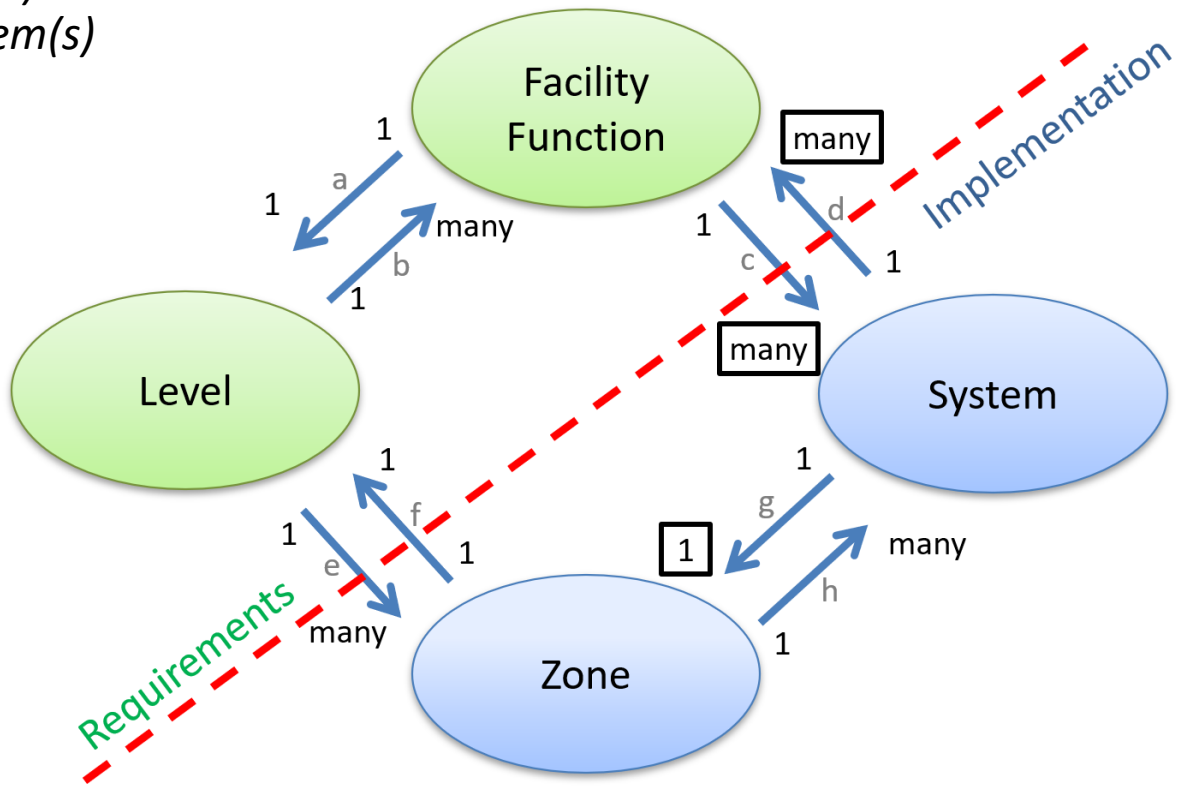
Attack Model

- By exploiting a vulnerability, adversaries can compromise the Confidentiality, Integrity, Availability of an Significant Digital Asset
- Goal: Affect function through compromise of system
- May result in impact (the undesirable event or consequence)



Relationships between Concepts

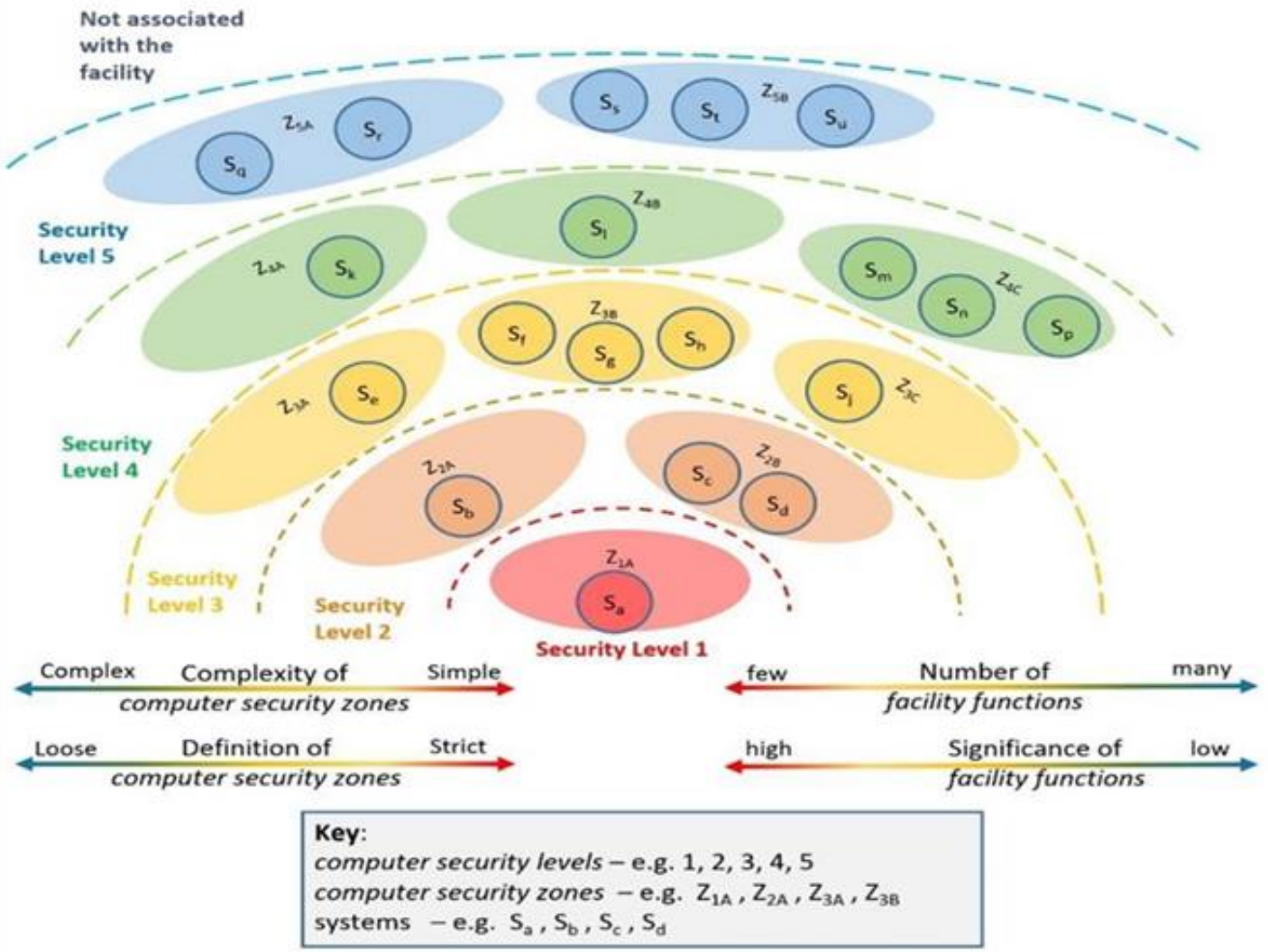
a – Each *Facility Function* is assigned to a single *Level*
b – Each *Level* may be applied to one or more *Facility Function(s)*
c – Each *Facility Function* may be assigned to one or more *System(s)*
d – Each *System* may perform one or more *Facility Function(s)*
e – Each *Level* may be applied to one or more *Zone(s)*
f – Each *Zone* is assigned a *Level*
g – Each *System* is placed within a single *Zone*, where possible
h – Each Zone may consist of one or more System(s)



National Nuclear Security Administration

DCSA and Zones

- An implementation artifact of a computer security program
- They can be directly observed (via physical boundaries) and determined using network security tools
- Systems inside a zone maintain trust relationships with each other



ORS Office of Radiological Security
Protect · Remove · Reduce

National Nuclear Security Administration

What is Ransomware?

- Ransomware is the payload of the attack
- Encrypts your documents
  - Then holds them for payment
- Ransomware malware can be purchased for about $50 on the dark web

ORS Office of Radiological Security
Protect · Remove · Reduce

How does it get in?

- Delivered by many different methods
  - 47% - Remote Desktop software vulnerabilities or brute force attacks (password guessing)
  - Virtual Private Network vulnerabilities or brute force attacks (password guessing)
  - 17% - Other vulnerable network services
  - 26% - Getting users to open phishing emails
  - Getting users to visit web sites with malware
  - 10% - Taking over user accounts
- May even be a non-automated attack (human hackers)
- The malware exploits some vulnerability in your computer system

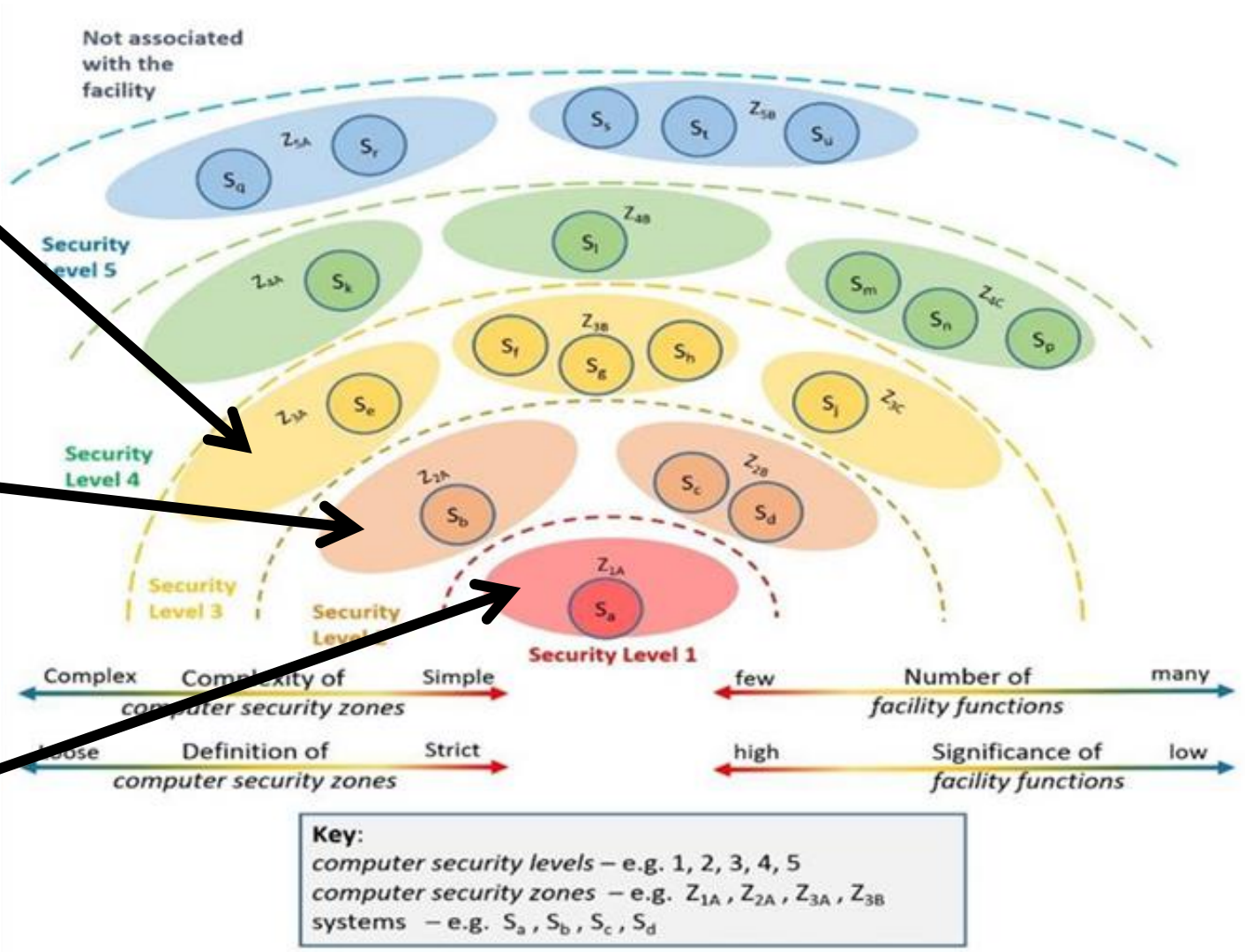
National Nuclear Security Administration

Potential DCSA

Zone C – Physical Protection Equipment (e.g., Access Control) at the Boundary

Zone B – PP Equipment inside the Boundary

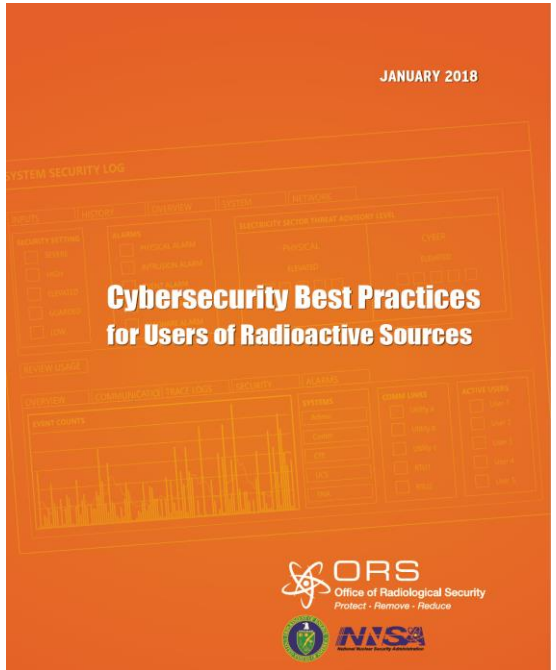
Zone A – Equipment controlling or storing the Source

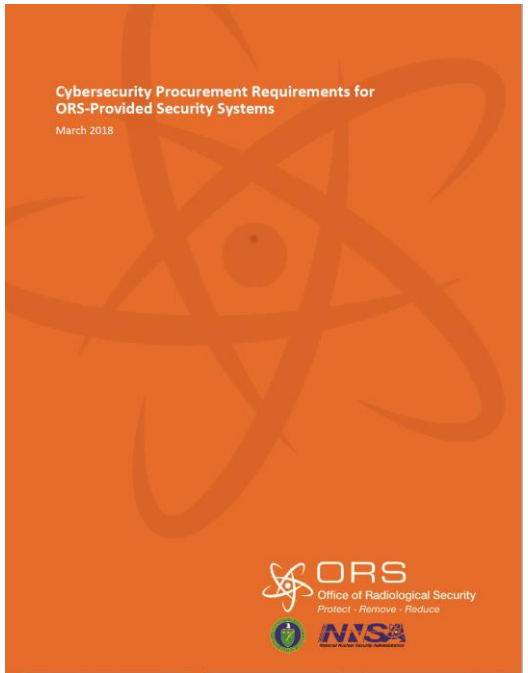


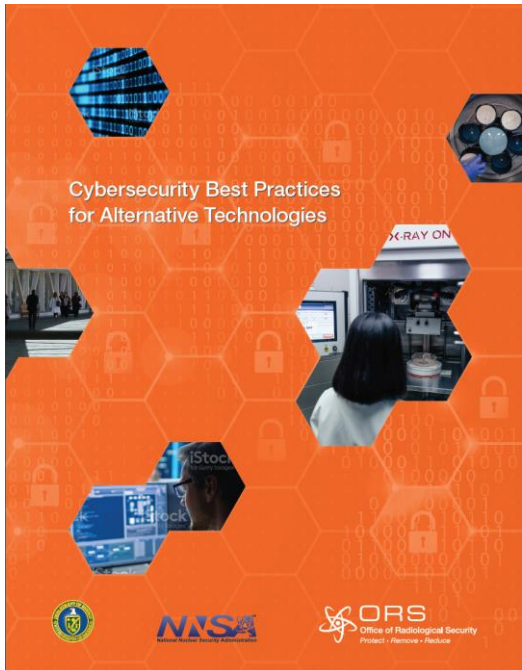
ORS Office of Radiological Security
Protect · Remove · Reduce

ORS Cyber Guides

- Cybersecurity Best Practices of Users of Radioactive Sources
  - Guidance on implementing a Cybersecurity Programme , Zones and Levels
- Cybersecurity Procurement Requirements for ORS Provided Security Systems
  - Good reference for relationships with vendors and contractors
- Cybersecurity Best Practices for Alternative Technologies







Questions?