WINS and iia Webinar on

# SECURITY OF GAMMA IRRADIATION FACILITIES USED FOR RADIATION PROCESSING

2nd September 2020 at 03:30pm CEST

World Institute for Nuclear Security

# OBJECTIVES OF THE WEBINAR

## Welcome and thank you for joining us!

## Today's objectives:

- ❑ Review the risk and the need for security
- ❑ Discuss physical security features and security management principles
- ❑ Highlight the importance of addressing the rapidly evolving cyberthreat
- ❑ Share experience of gamma irradiation industry expert
- ❑ Encourage all participants to adopt best security practice

# **WELCOME** from the **International Irradiation Association**

*'The Global Voice for the Radiation Processing Industry'*

**www.iiaglobal.com**

Martin Comben - General Manager, Gamma Irradiation

- **Gamma irradiation industry is highly engaged**
  - has an exemplary safety and security record

However…

- **Threats evolve**

- **Research shows:**
  - Measures to address human factors – **fall short**
  - Cybersecurity regulations are not keeping pace with the **cyber** threat

# Agenda

- ❑ **Designing and Implementing Operational Security Measures at Gamma Irradiation Facilities**

**David Jackson**
Senior Radiation Safety Manager
Steris Applied Sterilization Technologies (AST)

- ❑ **Credible Threat**

- ❑ **Operators experience & perspectives**

- ❑ **Cybersecurity Best Practice**

**Brandon Gorton**
Cybersecurity Task Lead
& Principal Investigator
Pacific Northwest National Laboratory

**Derek Higgins**
Regional Project Manager
Pacific Northwest National Laboratory

# Panel of Experts

**Andreas Ostrowicki**
Managing Director, Beta-Gamma Service GmbH & Co. KG (BGS)

**Cherin Balt**
Managing Director, High Energy Processing Cape (Pty) Ltd (HEPRO)

**Doug Day**
Physical Protection Expert, Pacific Northwest National laboratory (PNNL)

- Please ask questions and participate in the E-voting

# Some Housekeeping items

There are 4 tabs on the top of your screen ("Chat"; "Questions"; "Polls" and "People"):

- Feel free to use the "**Chat"** option to share any insight you may have
- You can type and submit your questions through the "**Questions"** tab. Any questions which we are not able to answer during the webinar due to time limitations will be consolidated and answered after the webinar.
- We will have several voting questions during this webinar. You can access the voting questions from the "**Polls**" tab and then close the window to return to the slides. We will be discussing 3 of them as introduction to the presentations or particular topics to further explore. The last one will be used at the end of the webinar to assess your satisfaction.
- Finally, you will be able to see who else is participating by clicking on the "**People**" tab.

The webinar will be recorded for future viewing and will be made available in the Members Area of the WINS website

## E-Voting

1. What type of organisation do you work for?

2. How credible is the threat to rad sources used for gamma irradiation?

3. I believe that security arrangements implemented at gamma irradiators are sufficient and effective

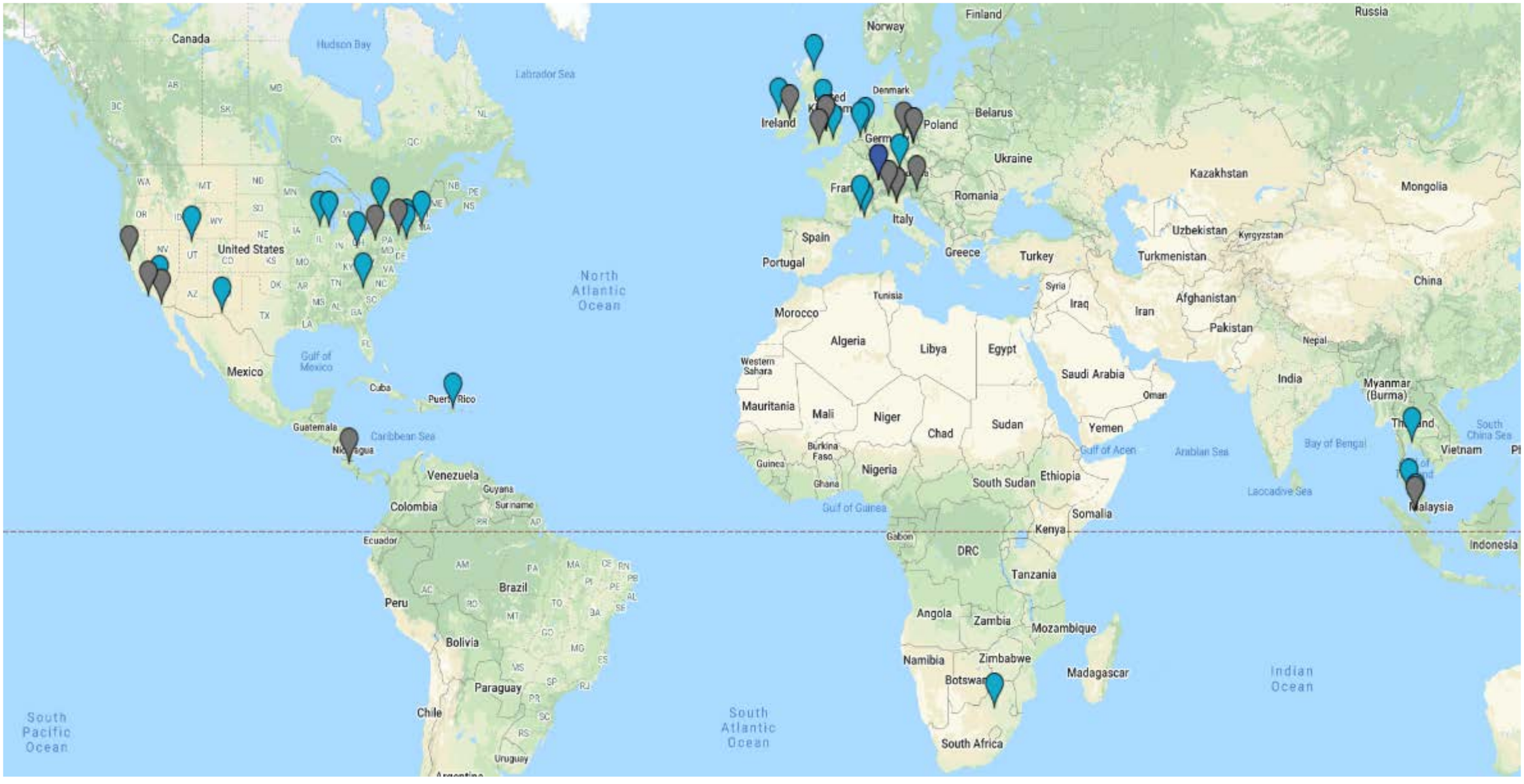
# Designing and Implementing Operational Security Measures at Gamma Irradiation Facilities

*Presented By: David M. Jackson, CIH, Sr. Radiation Safety Manager – STERIS AST - Americas*

STERIS

Applied Sterilization Technologies

# STERIS AST - America



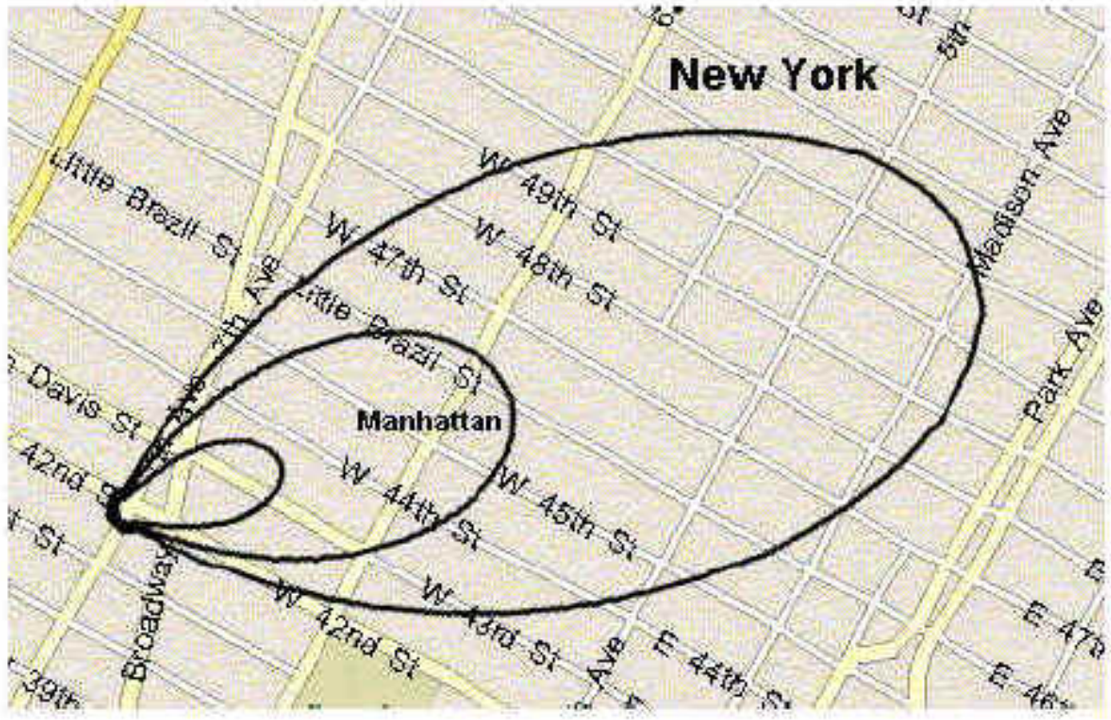

www.steris-ast.com

STERIS
Applied Sterilization Technologies

# The Concern Remains Valid


Lost or stolen material will be used maliciously by terrorist groups as an RDD or RED within a populated area

**Figure 4: Immediate Effects Due to Americium Bomb in New York City**




| | |
|---|---|
| **Inner Ring:** | All people must receive medical supervision |
| **Middle Ring:** | Maximum annual dose for radiation workers exceeded |
| **Outer Ring:** | Area should be evacuated before radiation cloud passes |

STERIS
Applied Sterilization Technologies

# Target of Concern

Source Racks come in variety of sizes and configurations

Pool Depth: 20-25 ft  (6-7.6 m)

Activity:
  Source:  11,000ci new  (407 TBq)
  3000-5000ci avg. (111-185 TBq)

  Module:  150kci – 230 kci  (5.6–8.5 PBq)

  99.9% are Category 1

Self Protecting
  Co60 Gamma Constant: 1.3 R/hr/ci at 1m

  Time to 1000R (10Sv)
    11,000 ci source:  4.2 minutes
  200,000 ci Module:  14 seconds

≈ 3.50 Mci  (129 PBq)

STERIS
Applied Sterilization Technologies

# Global Framework

- International Atomic Energy Agency
  - 8-G - “Preventive and Protective Measures Against Insider Threats”
  - 11-G - “Security of Radioactive Material In Use and Storage and of Associated Facilities”
  - 37-G – “Developing a National Framework for Managing the Response to Nuclear Security Events”
- WINS
  - Also has a number of Documents
    - 1.4 – “Nuclear Security Culture”
    - BPG 5.8 – “Security of Radioactive Sources Used in Industrial Radiation Processing”
- Nation States
  - Could be general or very specific.
  - US NRC

STERIS
Applied Sterilization Technologies

# Insider Threat

**Insiders have knowledge about;**

- Targets
  - Locations, quantities
  - Details about facility
- Security
  - Location and details about the system
  - Details about protocols
- Operations
  - Tools and equipment
  - Processes
  - Materials
  - Alarms and alerts

**Insiders;**

- Can have Authority over people
  - Designated Authority
  - Personal Influence
- Control or Influence
  - Alarm assessments
  - Sensitive information
  - Procedures and Processes
- Knowledge
  - Tools and equipment location
  - Alarm protocols or overrides

STERIS
Applied Sterilization Technologies

# Access Authorization

**Background Check**

- Verification of Identity
- Local Criminal History
- Character Reference Check

**FBI Criminal History Check**

- Fingerprints
- Criminal History
- Identification

**Trustworthy and Reliability Assessment**

for Unescorted Access to the Radioactive Material and Access to Protected Information by Reviewing Official

**Job Classifications Requiring T&R**

- Operators
- Supervisors
- Maintenance Technicians
- Operations Administrators

STERIS

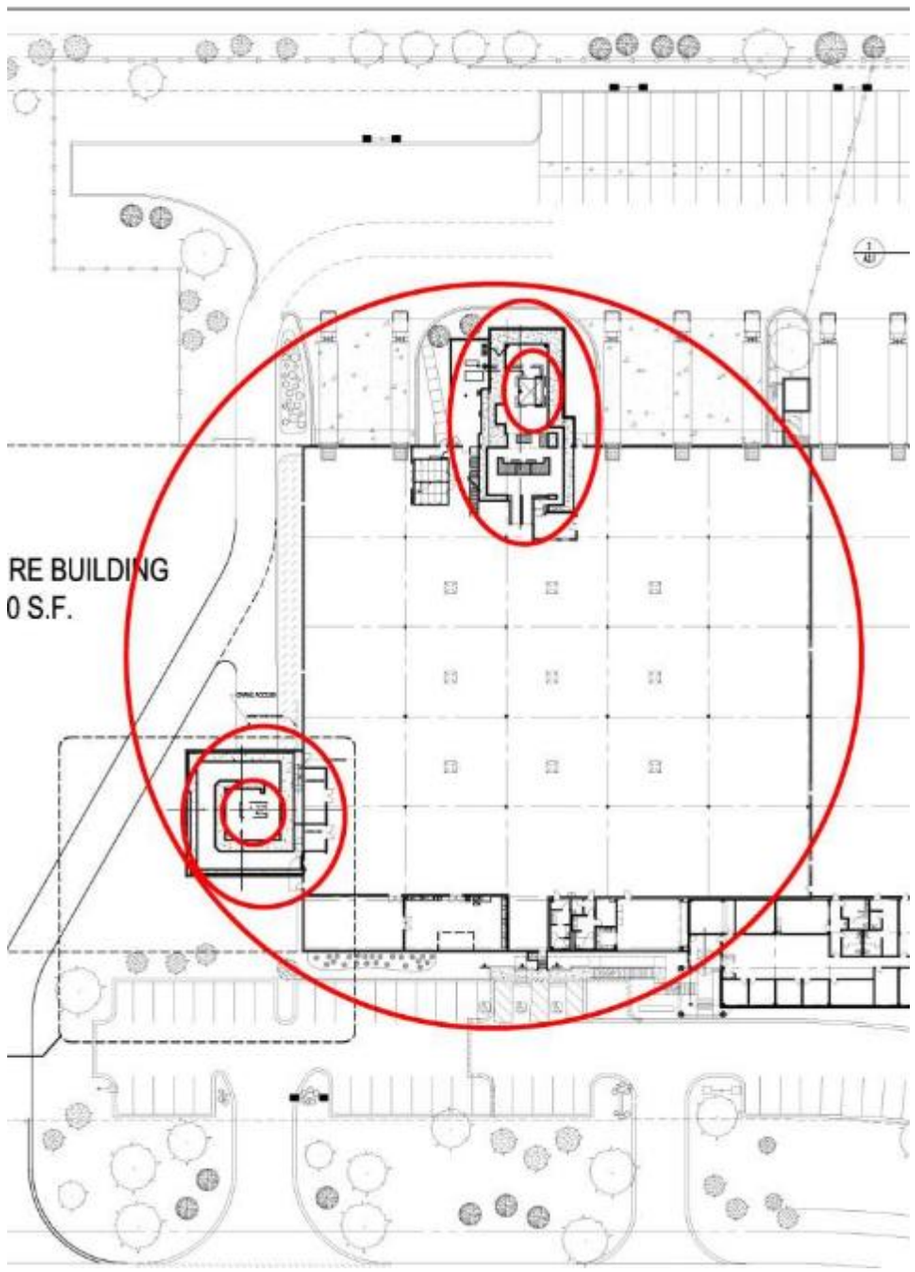
Applied Sterilization Technologies

# Access Control – Security Zones

Define the **Security Zone**
- Continuous Physical Barrier
- Entry thru Access Control Points
- Unescorted access only by T&R individuals
- Maintain direct control
    - Continuous surveillance
    - Intrusion Detection Devices

Establish **Temporary Security Zones** during periods of Maintenance
- Source Receipt and Handling

Coordinate with Local Law Enforcement for a timely armed response




STERIS
Applied Sterilization Technologies

# Access Control – Outer Perimeter

- Perimeter Fencing with barbed wire
  - Man gates allow egress only
  - Truck gates are locked after scheduled pickup and delivery hours
  - Truck gates monitored by camera or personnel

STERIS
Applied Sterilization Technologies

# Access Control – Middle Perimeter

- Building
  - Controlled Access entrance points into the building for  Employees, Visitors, and Contractors
  - Limited Access points & maintain the access
  - Truck drivers should not have access to the building unless escorted

STERIS
Applied Sterilization Technologies

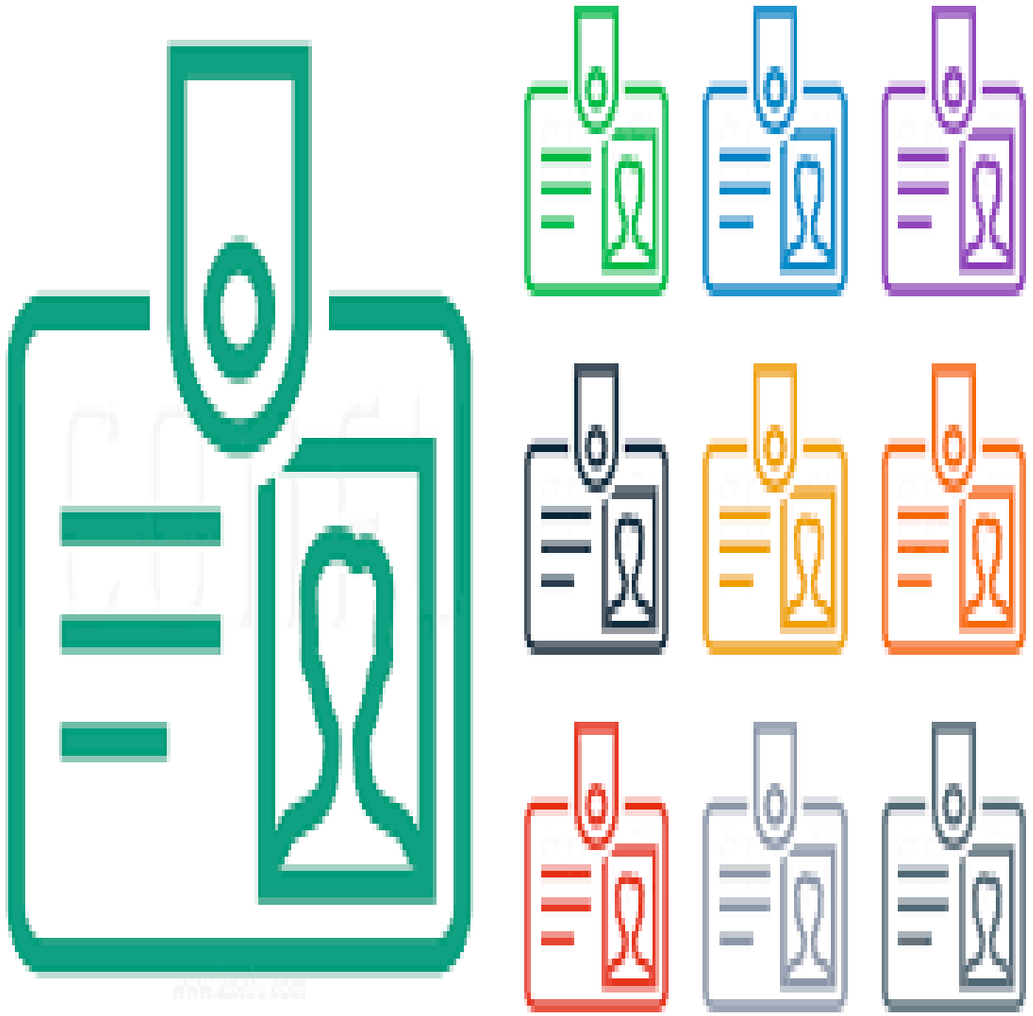
# Access Control – Middle/Inner Perimeter

- Building
  - Autodial intrusion alarm system for each designated Security Zone
  - Redundant means of Communication to the Alarm Service Company


STERIS
Applied Sterilization Technologies

# Access Control – Middle/Inner Perimeter

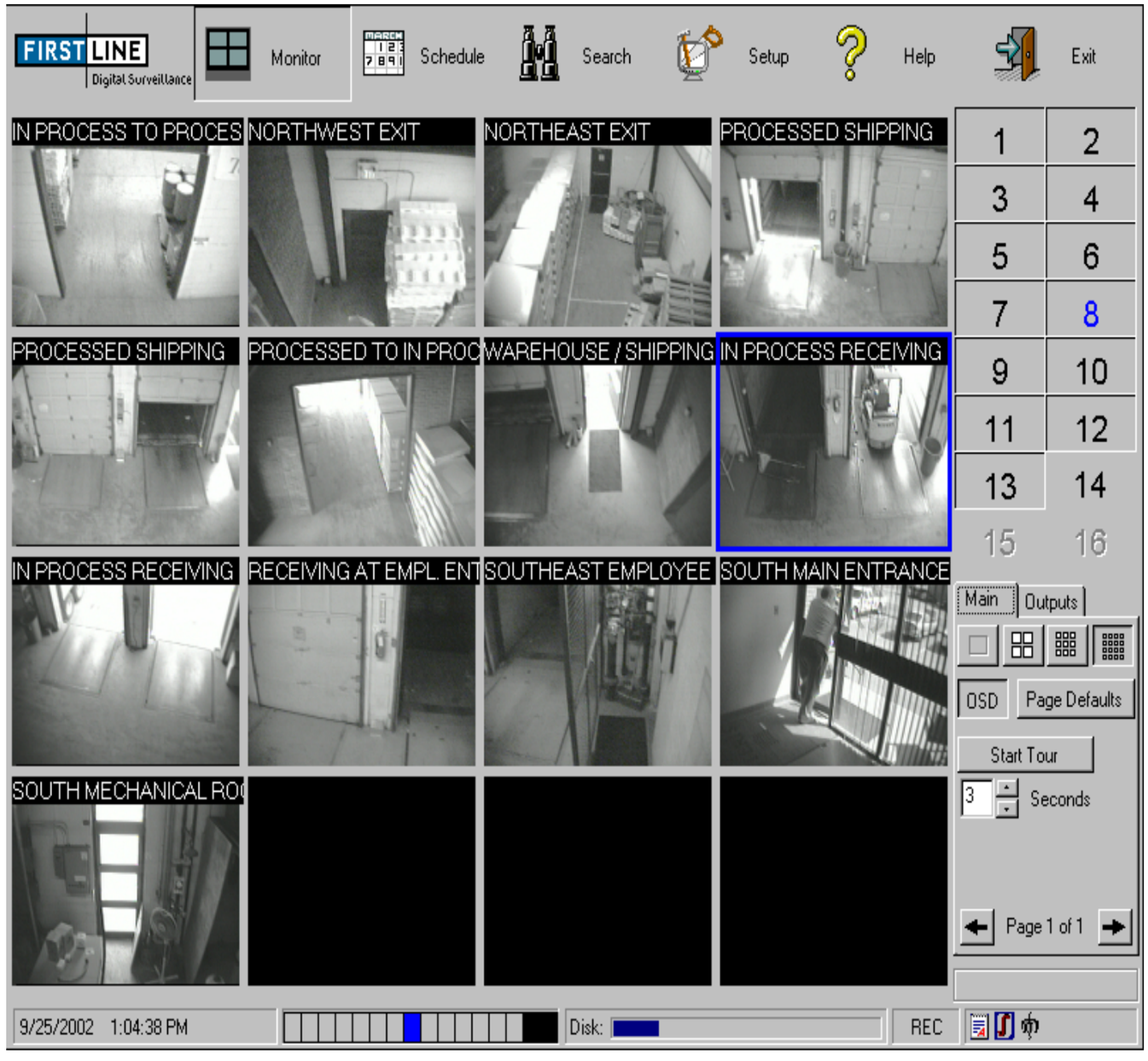
- Employee Photo ID Badge
  - Programmable Proximity Badge allows access only through authorized control points
    - Employee Badge always worn in plain site
    - Allows access only to where needed
- Contractors with an acceptable T&R assessment may also be issued a temporary ID badge
  - Allows access only to where needed
  - Need to be programmed for only the time period needed.



STERIS
Applied Sterilization Technologies

# Multi-Layered Approach to Access Control

- Building
  - All perimeter doors and critical internal doors and openings are under continuous CCTV surveillance
  - System used to verify the validity of any incident
    - Simple B&E or attempt to access RM?
  - Remote viewing access (minimum 30 days)




STERIS
Applied Sterilization Technologies

# Detection – Inner Perimeter

- **Detect without delay Unauthorized Entry into the Security Zone**
  - Continuous surveillance during normal operations
  - Intrusion Detection Sensors during shutdown periods

Motion Sensor


Radiation Monitor


Entry Door Contacts

Glass Break Sensor

STERIS
Applied Sterilization Technologies

# Physical Security - Delay

- Pool Covers and Shrouds

STERIS
Applied Sterilization Technologies

# Physical Security - Delay

- Stronger Doors and Locks


STERIS
Applied Sterilization Technologies

# What You Don’t Know

## Access to Professional Security Knowledge

- Work closely with your Security Staff
- Work closely with Local Law Enforcement
  - Drills? Tours?
- Government
  - The Office of Radiological Security

Office of Radiological Security
*Protect · Remove · Reduce*

STERIS
Applied Sterilization Technologies

# *Thank You*

STERIS
Applied Sterilization Technologies

# THREATS

- How Credible is the Threat?
- What are possible scenarios of concerns?
- Can we consider radioactive sources used in gamma irradiators as “self-protected”?
- Questions from the audience?

# PANEL DISCUSSION

- How does David's presentation resonate to you? What is similar? What is different, especially for smaller organisations?
- Would you have examples of challenges you faced while strengthening the security of your facilities? Could you share with us how you have solved these challenges?
- Is it a problem to find suppliers that can meet the particular requirements of gamma irradiator security?
- Do you feel that regulation of gamma irradiators in your country is clear and appropriate?
- What would be your top advice to a security manager willing to improve the security of his/her facility?

- **Questions from the audience?**

ORS
Office of Radiological Security
*Protect · Remove · Reduce*

# Cybersecurity Best Practices

PNNL-SA-155371

## September 3, 2020


**Derek Higgins, PMP | EVP**
*Derek.Higgins@pnnl.gov*
Office: 509-371-6602

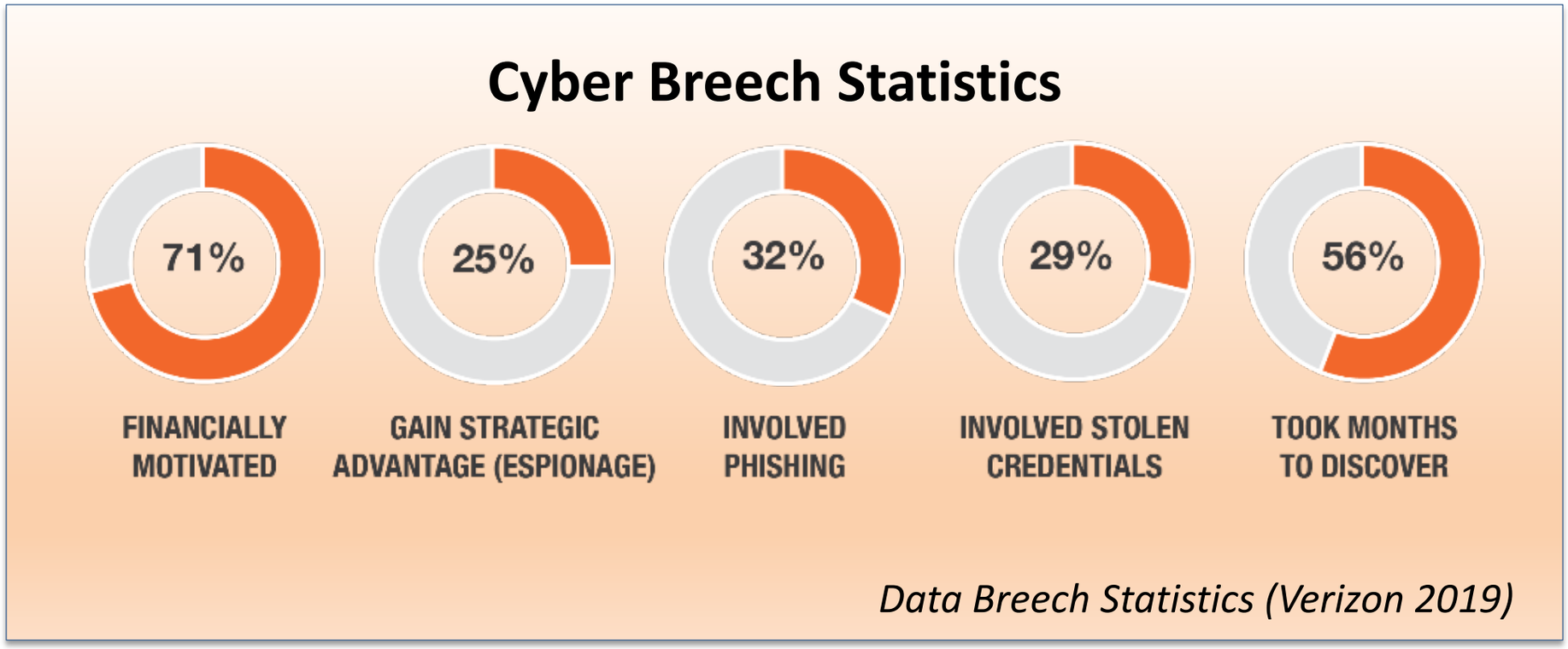
**Brandon Gorton, PSP | CISSP**
*Brandon.Gorton@pnnl.gov*
Office: 509-375-4517



National Nuclear Security Administration
Global Material Security

# Objective

- Provide the background/purpose of ORS and its role in promoting cybersecurity
- Suggest two major best practices with tangible ways to improve cybersecurity at radiological facilities

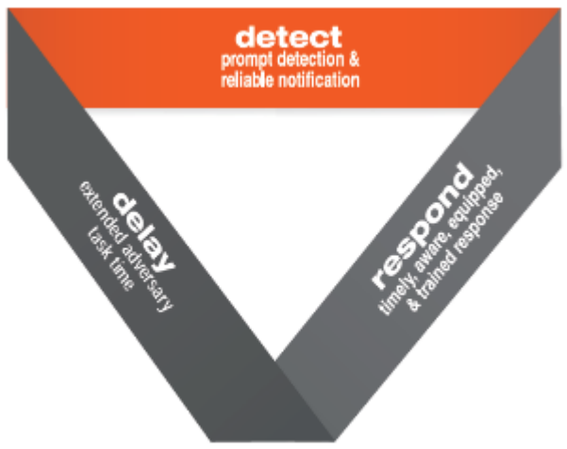



*Data Breech Statistics (Verizon 2019)*

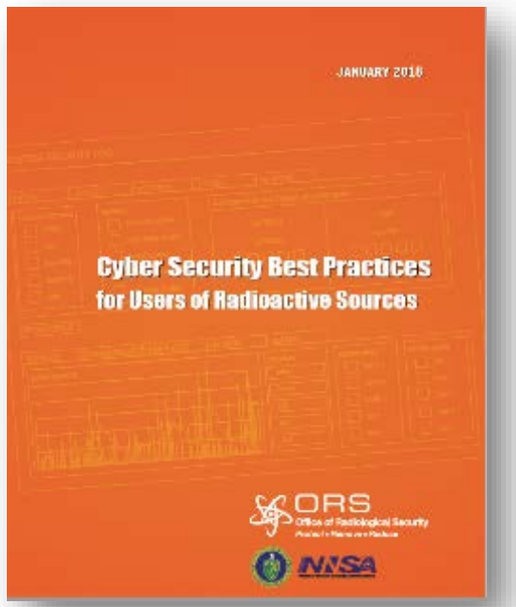
# ORS Background

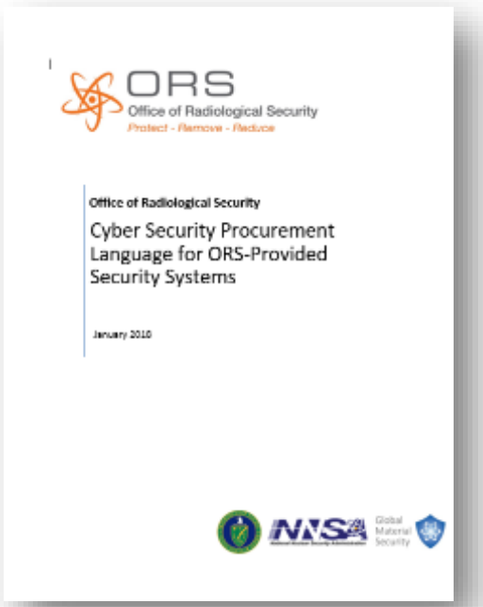
***ORS's mission is to enhance global security by preventing high-activity radioactive materials from being used in acts of terrorism***

- **Protect** radioactive sources used for vital medical, research and commercial purposes
- **Remove** and dispose of disused radioactive sources
- **Reduce** the global reliance on high-activity radioactive sources




*Security Protection Elements*



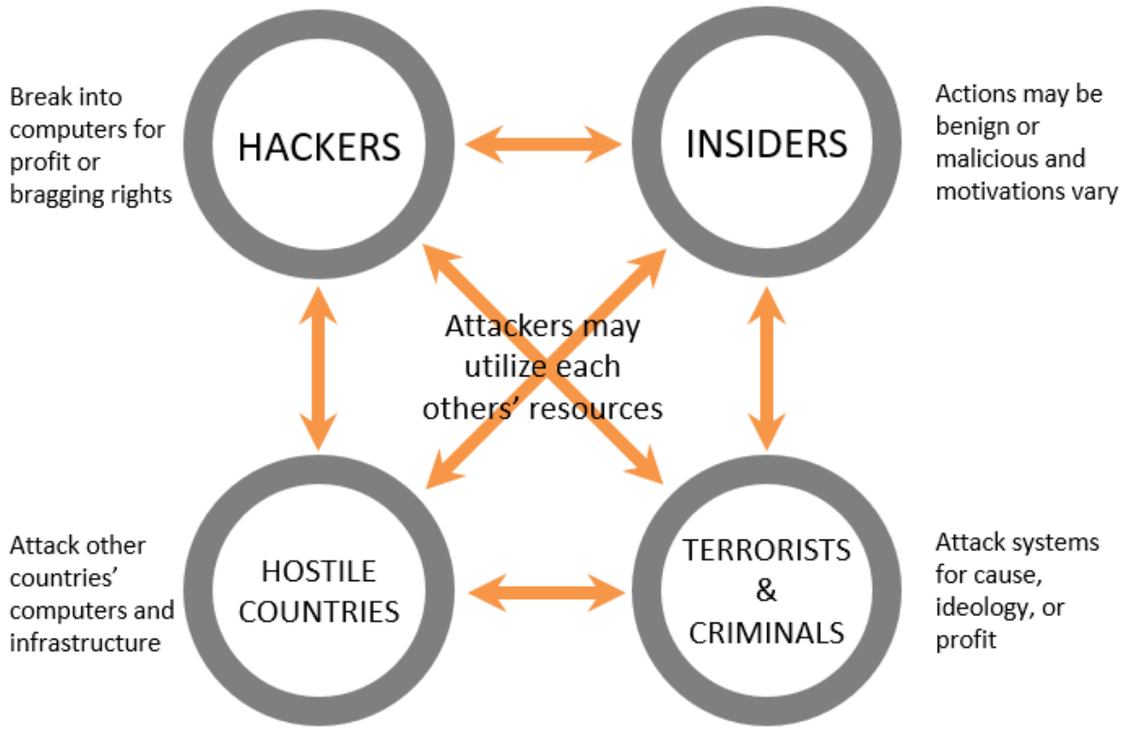




National Nuclear Security Administration

Global Material Security

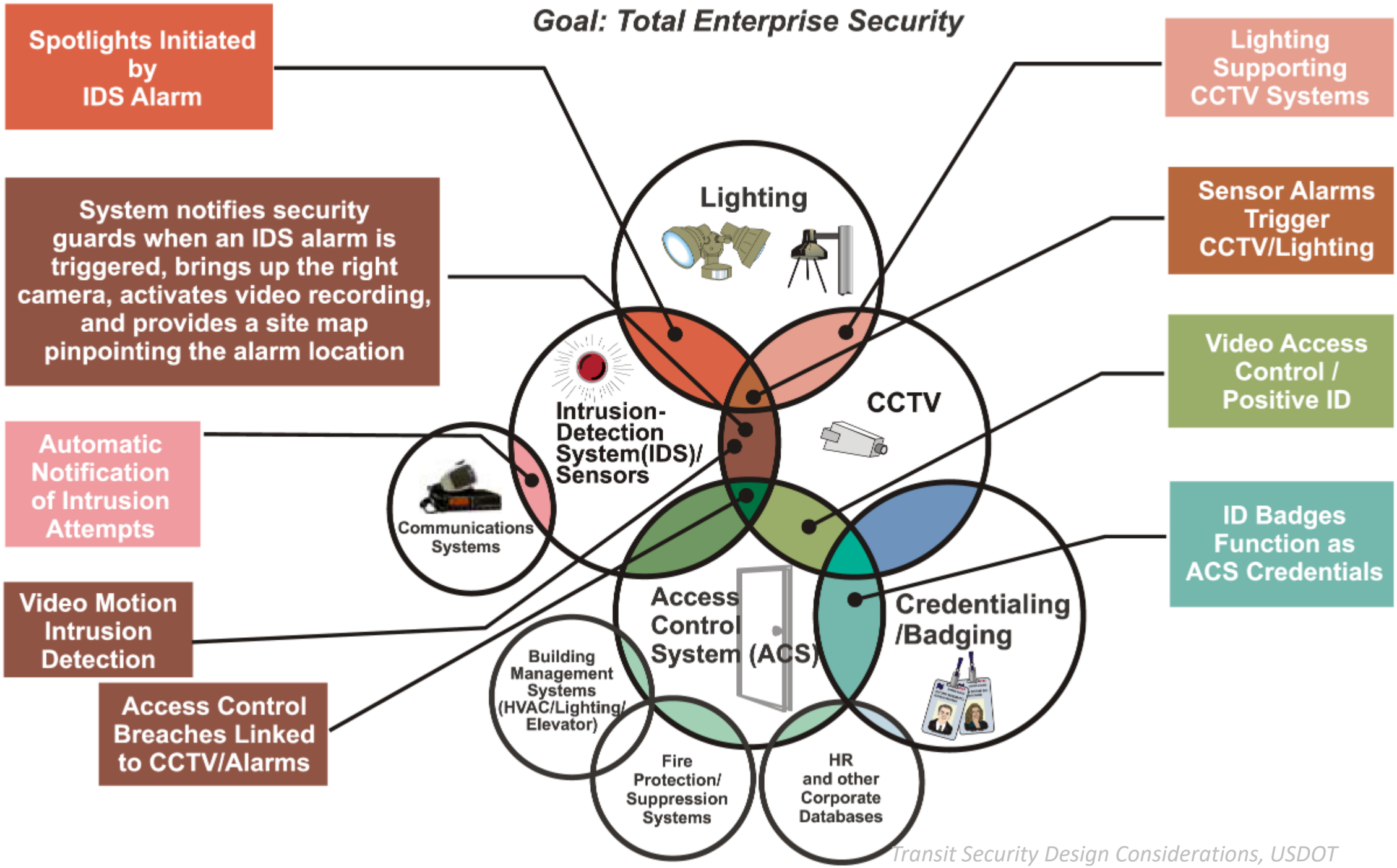
# Radioactive Sources and Cybersecurity

- The Threat
  - The compromise of a site's network controls and physical security measures, facilitating an attack on radioactive source
  - The compromise of a site's security equipment to gain access to a site's network
  - The use of social engineering to gain access to a site's physical security systems and networks



ORS
Office of Radiological Security
*Protect · Remove · Reduce*

# Radioactive Sources and Cybersecurity




*Transit Security Design Considerations, USDOT*

National Nuclear Security Administration
Global Material Security

# Reduce the attack surface – Managers

*(Strategic/policy level)*

1. Defense in depth and layered protection architectures

   *Concentric layers of security around an asset*

2. Principle of least privilege

   *Access is not afforded to those who do not need it to perform their duties*

3. Cyber hygiene practices

   *Can be defined as the practices or actions taken by owners and users to maintain the health and security of electronic information.*

   *These actions are often routine and help to mitigate data from being lost to nefarious and unintentional loss or corruption*

# *Reduce the attack surface – Employees*

*(Operational/device level)*

1. Defense in depth and layered protection architectures
   - Implement network segmentation and isolation
   - Full disk encryption

2. Principle of least privilege
   - Remove unnecessary software from workstations
   - Manage account and resource access levels

3. Cyber hygiene practices
   - Keep software up-to-date
   - Close excess ports and disable unused protocols on network appliances
   - Eliminate complexity whenever possible (e.g., unused, redundant, or duplicate rules)
   - Maintain routers, firewalls, and switches appropriately
   - Promote vigilance of connectivity (Wi-Fi and Bluetooth) – Bring your own device
   - Educate about the risks of external data exchange – EMAILS!
   - Continuous effort

# *Ensure integrity of security-related devices and communications – Managers/Policy*

*(Strategic/policy level)*

1. Account management

   *Oversight and governance of user credentials. Frequently involves creation of new accounts, modification of existing, and closure of accounts no longer requiring the prescribed level of access*

   *Often enforced through access control models (e.g., role-based, rule based, among others)*

2. Authentication processes

   *Taking steps to reasonably assure that a user identify is valid*

# *Ensure integrity of security-related devices and communications – Employees*

*(Operational/device level)*

1. Account management
   - Mitigate privilege escalation
   - Enforce password management (utilize strong, unique passphrases)
   - Multi-factor authentication (MFA)
   - Continuous effort

2. Authentication processes
   - Validate integrity of hardware and software during installation and configuration
   - Secure access to infrastructure, virtual and physical devices (e.g., protecting admin and physical access via MFA)
   - Continuous effort

# Summary

***Radioactive material licensees can enhance the security of radioactive materials by implementing a balanced approach of physical security and cybersecurity***

- The digitalization of physical protection systems has created new attack pathways via networked systems
- All levels of the organization have a role to play in the implementation of a strong security culture
- Even advanced physical security and cybersecurity systems can be thwarted by failing to account for the human element

ORS
Office of Radiological Security
*Protect · Remove · Reduce*

# *Thank you for your time!*


**Derek Higgins, PMP | EVP**
**Derek.Higgins@pnnl.gov**
**Office: 509-371-6602**

**Brandon Gorton, PSP | CISSP**
**Brandon.Gorton@pnnl.gov**
**Office: 509-375-4517**


National Nuclear Security Administration
Global Material Security

# CYBERSECURITY

- Is it your experience that industries using radioactive sources are addressing the cyberthreat sufficiently?
- What one or two key actions will best protect he radiation processing industry from cyberthreat?
- Should we expect greater regulation or new standards (e.g. IAEA) in the future?
- Questions from the audience?

# I. RESPONDING TO A SECURITY INCIDENT

# II. DEVELOPING A ROBUST SECURITY CULTURE

# Responding to a security incident

## Poll question

- I believe effective response arrangements are in place in case of a security incident.

## Follow up discussion

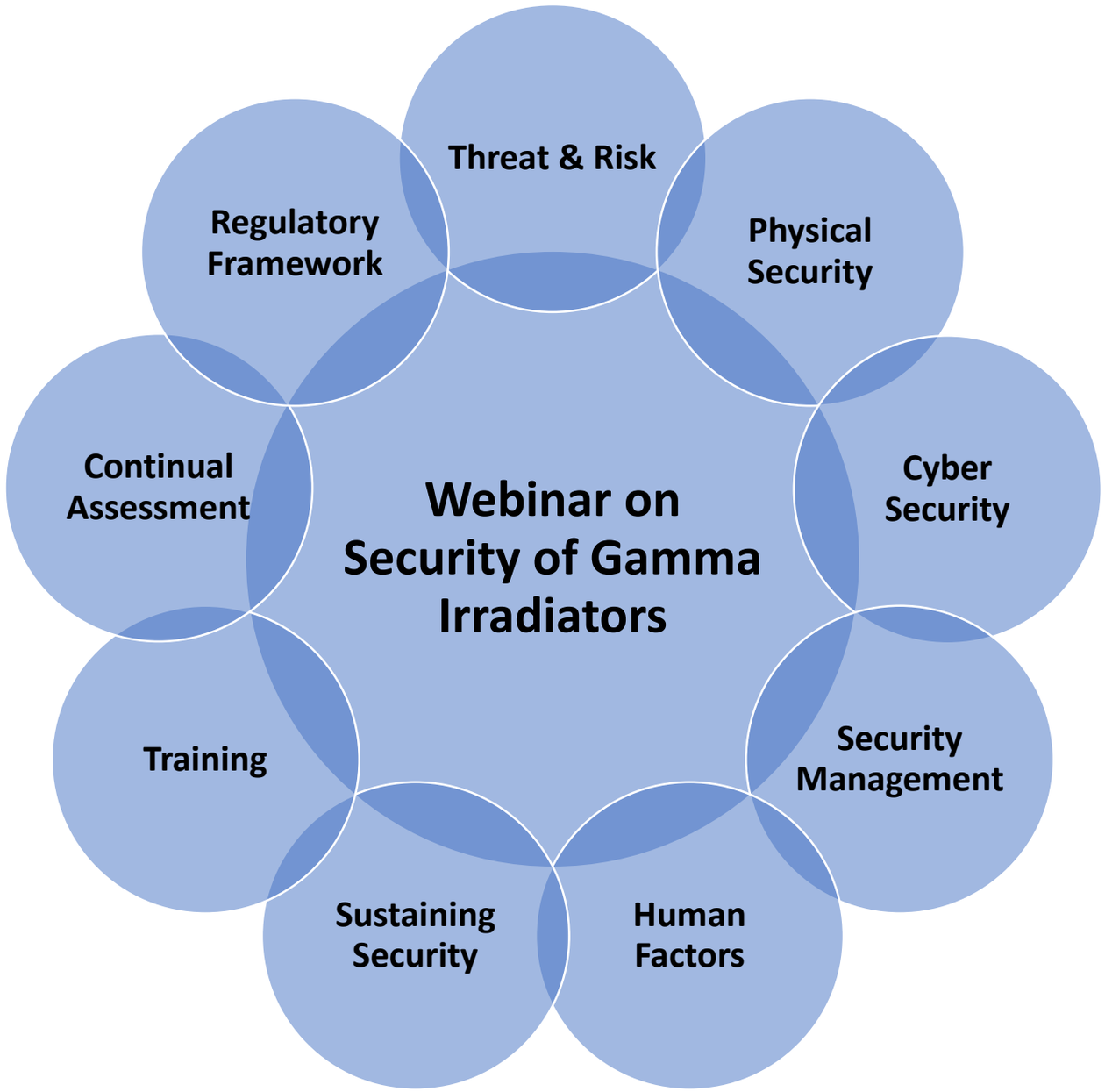
- What are the key elements of effective response arrangements?
- What are the usual challenges? How can we improve the situation?

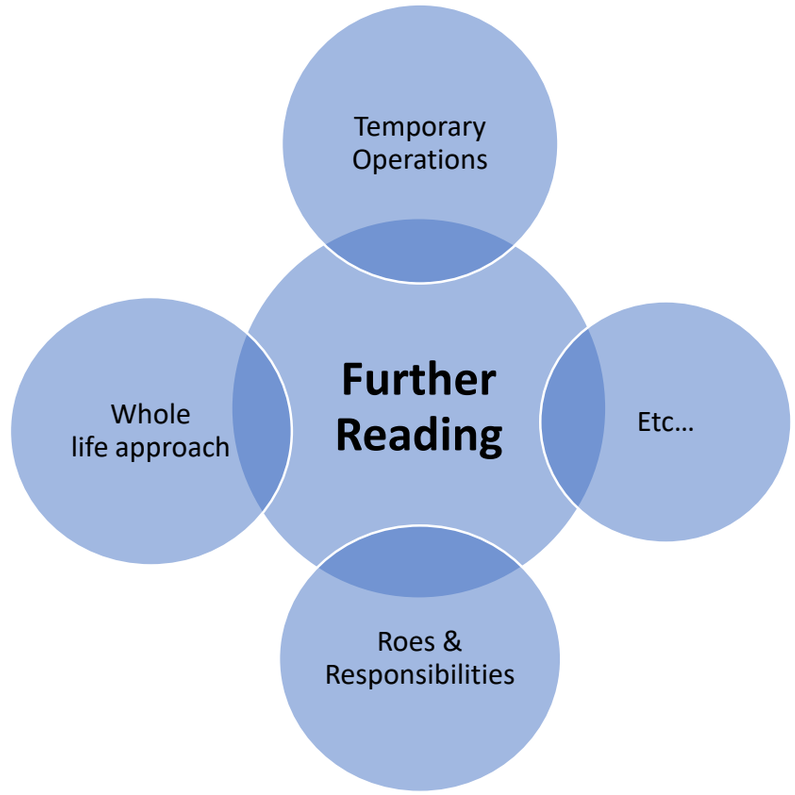
# Developing a Robust Security Culture

## Discussion

- Has the gamma irradiation industry developed a robust security culture?
- What are best practices for developing a sustainable security culture?
- How do you engage staff into security matters (awareness and education)?

# NEXT STEPS


Webinar on Security of Gamma Irradiators
Threat & Risk
Physical Security
Cyber Security
Security Management
Human Factors
Sustaining Security
Training
Continual Assessment
Regulatory Framework


Temporary Operations
Whole life approach
Further Reading
Etc…
Roes & Responsibilities

# FURTHER READING

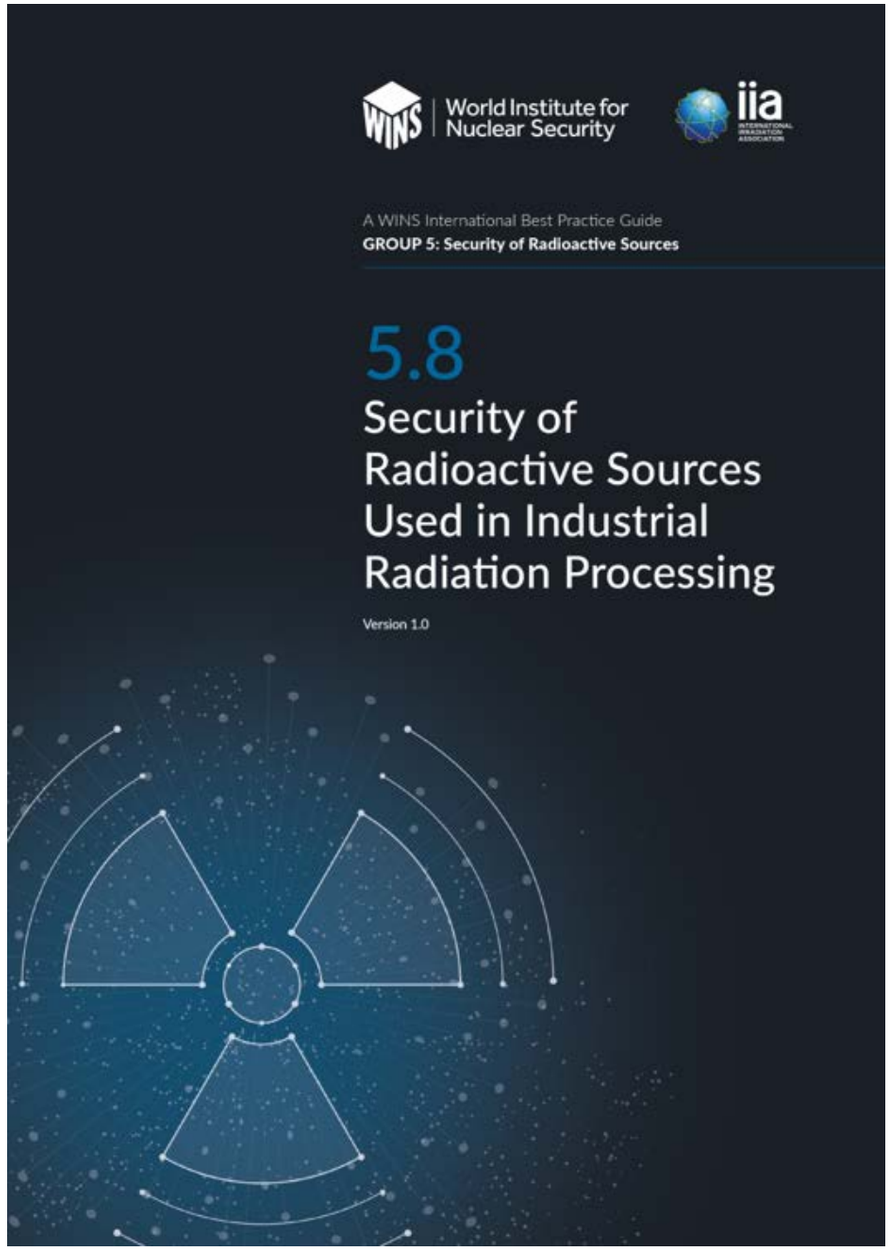
## Joint iia/WINS Best Practice Guide

Security of Radioactive Sources Used in Industrial Radiation Processing

Available at:

**www.iiaglobal.com** - Resources

**www.wins.org** - Knowledge Centre



# CONCLUSION

**Thank you everybody for having joined us here today!**

Please use the poll question to let us know if you liked the webinar

If you have any further questions or comments, please

**Contact us at info@wins.org or info@iiaglobal.com**

**Visit us at www.wins.org or www.iiaglobal.com**

WINS and iia Webinar on

# SECURITY OF GAMMA IRRADIATION FACILITIES USED FOR RADIATION PROCESSING

THANK YOU FOR YOUR PARTICIPATION !

World Institute for Nuclear Security