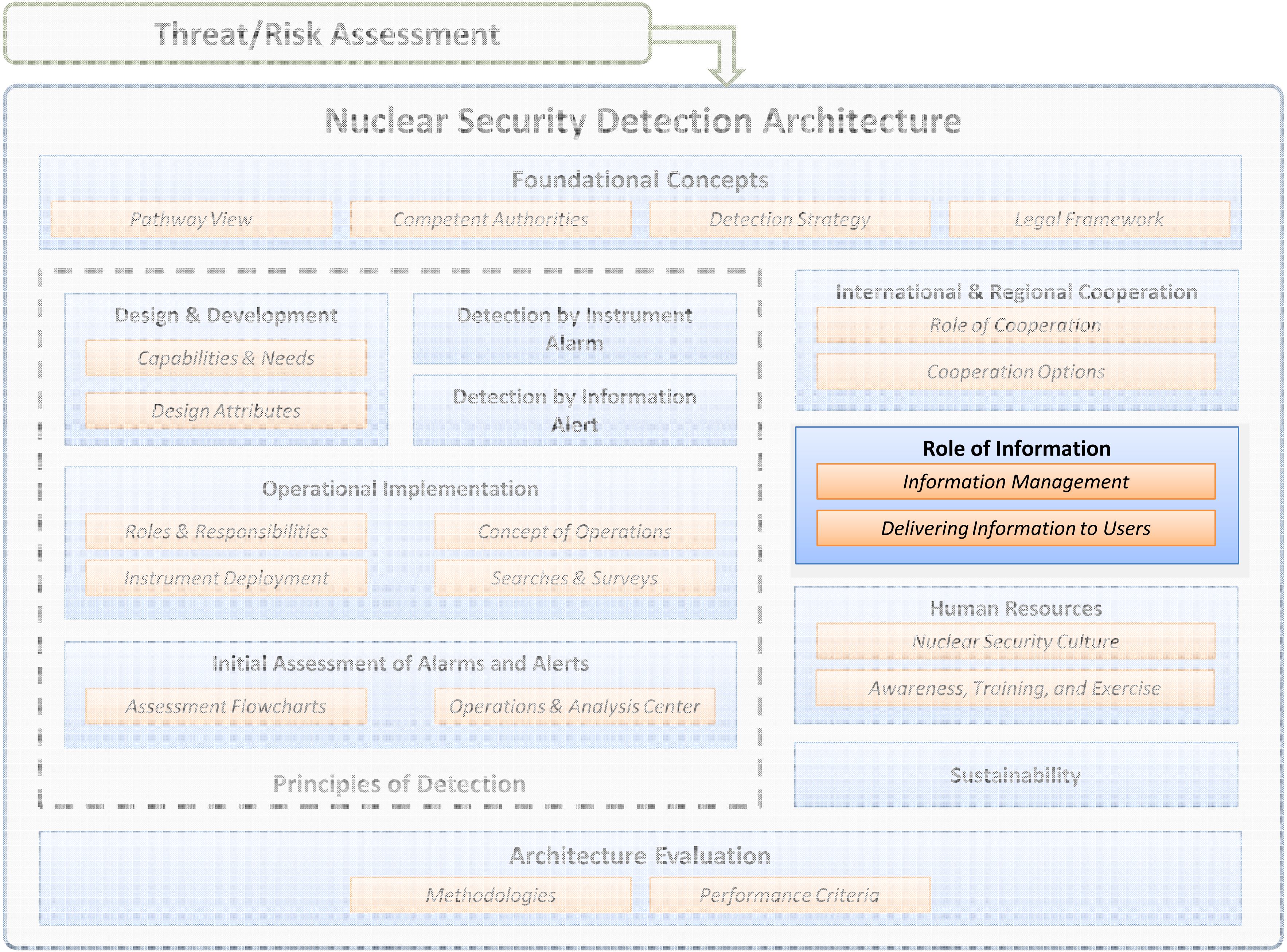
SAND2012-8185P

Role of Information in Effective Nuclear Security Detection

Nuclear Security Detection Architecture

Module K


Threat/Risk Assessment
Nuclear Security Detection Architecture
Foundational Concepts
Pathway View
Competent Authorities
Detection Strategy
Legal Framework
Design & Development
Capabilities & Needs
Design Attributes
Detection by Instrument Alarm
Detection by Information Alert
Operational Implementation
Roles & Responsibilities
Concept of Operations
Instrument Deployment
Searches & Surveys
Initial Assessment of Alarms and Alerts
Assessment Flowcharts
Operations & Analysis Center
Principles of Detection
International & Regional Cooperation
Role of Cooperation
Cooperation Options
Role of Information
Information Management
Delivering Information to Users
Human Resources
Nuclear Security Culture
Awareness, Training, and Exercise
Sustainability
Architecture Evaluation
Methodologies
Performance Criteria

Module Objectives

Participants will have an understanding of information management and the utilization of information for an effective nuclear security detection architecture, including:

- Sources and types of information
- Delivering information to users
- Information management

The information presented in this module is relevant to checklist questions:
29, 36, 39, 40, 41, 42, 43, 44, 45, 66

Role of Information in the Architecture

Information can be generated from many sources from within an architecture and can:

- Be used to detect, identify, and interdict material
- Identify suspicious activities
- Evaluate effectiveness
- Provide situational awareness

Information is vital for the implementation of an effective architecture

Sources of Information

Information can be generated throughout the architecture …

- Radiation instruments
- Other sensors
- Law enforcement
- Operational sources
- International partners

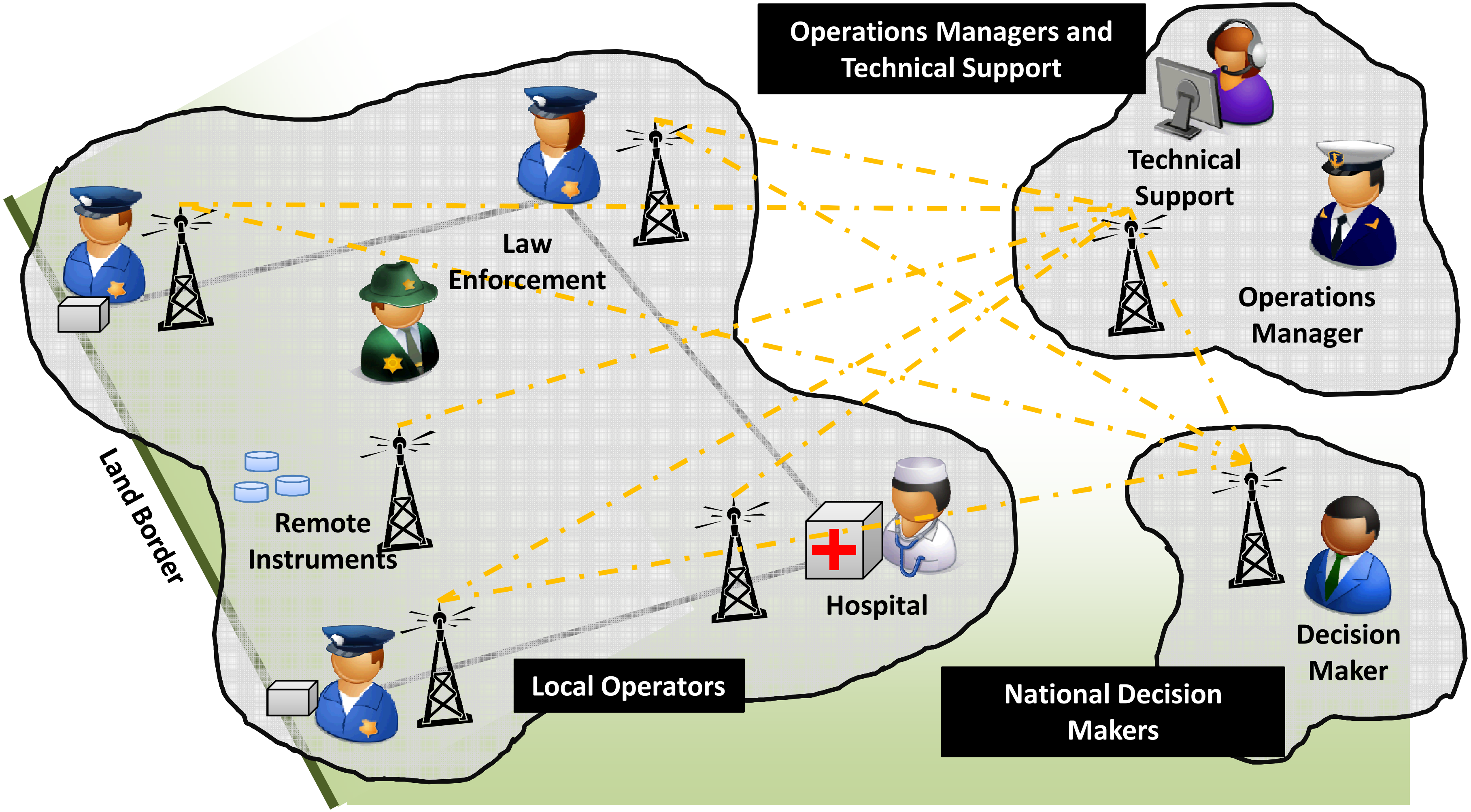
… and can come in different formats

- Raw Data
- Images
- Video
- Plain Text

Types of Information

	Threat and Alarm/Alert Information	Configuration Information	Status Information
	• Information on potential and actual nuclear security events • Information requires timely delivery to competent authorities	• Information on the setup and organization of detection assets • Assists operation managers and technical support	• Information on the current state of assets • Provides situational awareness • Enables a more rapid and effective response
Examples	• Nuclear security threat information • Detection events • Technical assessments	• Location of instrument • Instrument settings • Training and expertise of operators	• Instrument occupancy • Operational status

Delivering Information to Users



Data Exchange Protocols and Communication Infrastructure

- An effective architecture needs the ability to exchange accurate and timely data
- Architecture elements (such as instruments, technical support, and analysis centers) require an underlying communications infrastructure that is robust, redundant, and has sufficient bandwidth
- Data exchange protocols and common data formats enable stakeholders and instruments to transfer information in a standardized and structured way

Levels of Data Users

- Different users of information have varied requirements for content, presentation, and timeliness
- Creating a tiered structure for information flow is vital to assuring user data requirements are met

Providing correct data to the correct users at the correct time is necessary to ensure that information effectively supports the architecture

Example of Tiered Data Users

National Decision Makers

- Highest level data user
- Needs to receive information about nuclear security events
- Needs understanding of current capabilities and gaps

Operations Managers and Technical Support

- National and sub-national operations managers, leaders of operational agencies, and technical experts
- Typically manages real-time operations and situational awareness
- Requires secure and timely transfer to assist in assessment and technical support

Local Operators

- Typically the first and direct recipient of alarms and alerts
- Successful interdiction often requires quick decisions
- Requires rapid and easy to interpret information delivery to respond properly

Information Management

- Delivering data to users also requires that information be managed
- Information management can include:
  - Data storage and retention policies
  - Rules for disseminating information
  - The classification of sensitive information

Examples of Sensitive Information

Sensitive information is any information where the unauthorized disclosure, modification, alteration, destruction, or denial of use could compromise nuclear security

- Perceived national threats and vulnerabilities
- Results of the national threat and risk assessment
- Location and configuration of detection systems
- Operating procedures, including preparedness and response
- Communication, authentication, and encryption codes

Protection of Sensitive Information

Policies and procedures for the protection of sensitive information include:

- Classification of information according to national requirements
- Proper preparation, identification, and markings
- Appropriate encryption methods for storage and transmission
- Declassification of information when obsolete or no longer sensitive
- Proper destruction of data and documents

Additional Roles for Information

There are many other roles for information beyond those presented here, for example:

- Interfacing with the public
  - Public can generate alerts
  - Receiving information during a nuclear security event
- International cooperation
  - Sharing of operational information
  - Reporting to international agencies

Case Study

DATA EXCHANGE FOR ARCHITECTURES

Data Exchange Case Study

Challenge:

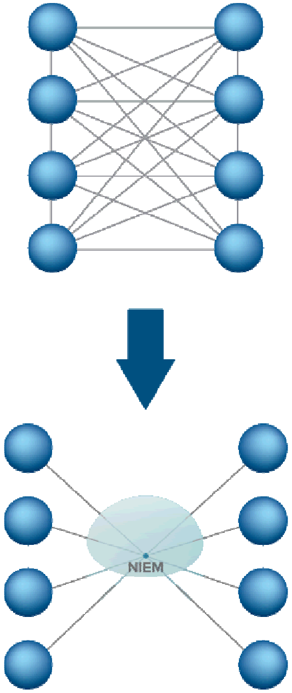
- U.S. architecture has thousands of sensors planted for chemical, biological, and nuclear detection
- Instruments use disparate message standards, syntaxes, and formats
- Message platforms range from email to telephone to fax
- Humans in the loop introduce opportunities for errors

Leveraging NIEM

- The US's National Information Exchange Model (NIEM) provides a common vocabulary for consistent, repeatable exchanges of information between agencies and domains
- NIEM allowed for architects to create a common data exchange protocol for radiological and nuclear messaging
- Data outputs from sensors would be unique to the type of sensor, but information around the file would be the same
- This enabled the structured transmission and interpretation of relevant data and machine-to-machine communication

NIEM

NATIONAL INFORMATION EXCHANGE MODEL



Piloting Data Exchange

- The protocol was successfully piloted in a 2008 exercise simulating a sensor network attempting to detect radioactive material
- Data messages were automatically passed from the sensors to an operations center and then to technical experts (previously this was done by email)
- Proved that data could be sent quickly and accurately from disparate devices, removing human errors, and improving the effectiveness of the architecture

For more information: http://ise.gov/sites/default/files/DNDO-Brochure_20110705.pdf

Module K

DISCUSSION QUESTIONS

Discussion Questions

1. What are the benefits and challenges of retaining data for later analysis? How can this lead to a more effective architecture?
2. What are some challenges in dealing with different sources and types of information? How can these problems be overcome?
3. Assuming the tiers of data users discussed in this module, describe the requirements that each group has on information with regards to:
   - **Type of data** (raw data from instruments, system health data, historical patterns, etc.)
   - **Quantity** (access to all data, portions of data, etc.)
   - **Timeliness** (time to receive data)
   - **Presentation** (the complexity and clarity of how the data is presented)
4. Are there other ways to tier data users within the architecture? If so, how does that affect the requirements in Question 3)