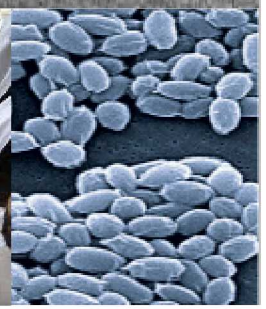
SAND2020-8067PE

DHS Chemical & Biological Defense Architecture Development Overview

David Shepherd
S&T Directorate, DHS

Patricia Hernandez, Nataly Beck, Benjamin Bonin, Trisha Miller, Janson Wu
Sandia National Laboratories

This work was funded under Contract No. HSHQPM-17-X-00236 awarded to Sandia National Laboratories by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T).

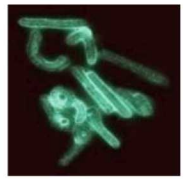
Background and Context

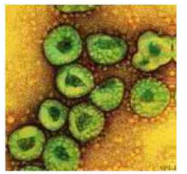
- Effort began in 2016 to map the chemical and biological defense space, including the functions and organizations within it
- A systems architecture approach was used to describe the complex system
- Goals of the architecture include:
  - Traceability to original policy and mission space
  - Communication tool for partners and policy makers
  - Mapping of interdependencies, priorities, and gaps
  - Inform decision making and program development

The architecture can provide a framework for mapping organizations and tracing capabilities to enable better preparedness and response to national security events

Chemical and biological defense is a complex national, state, and local enterprise.

- Diverse and evolving threats
- Numerous public and private stakeholders with overlapping interests and authorities
- Multitude of potential technical and non-technical capabilities for prevention, detection, and response





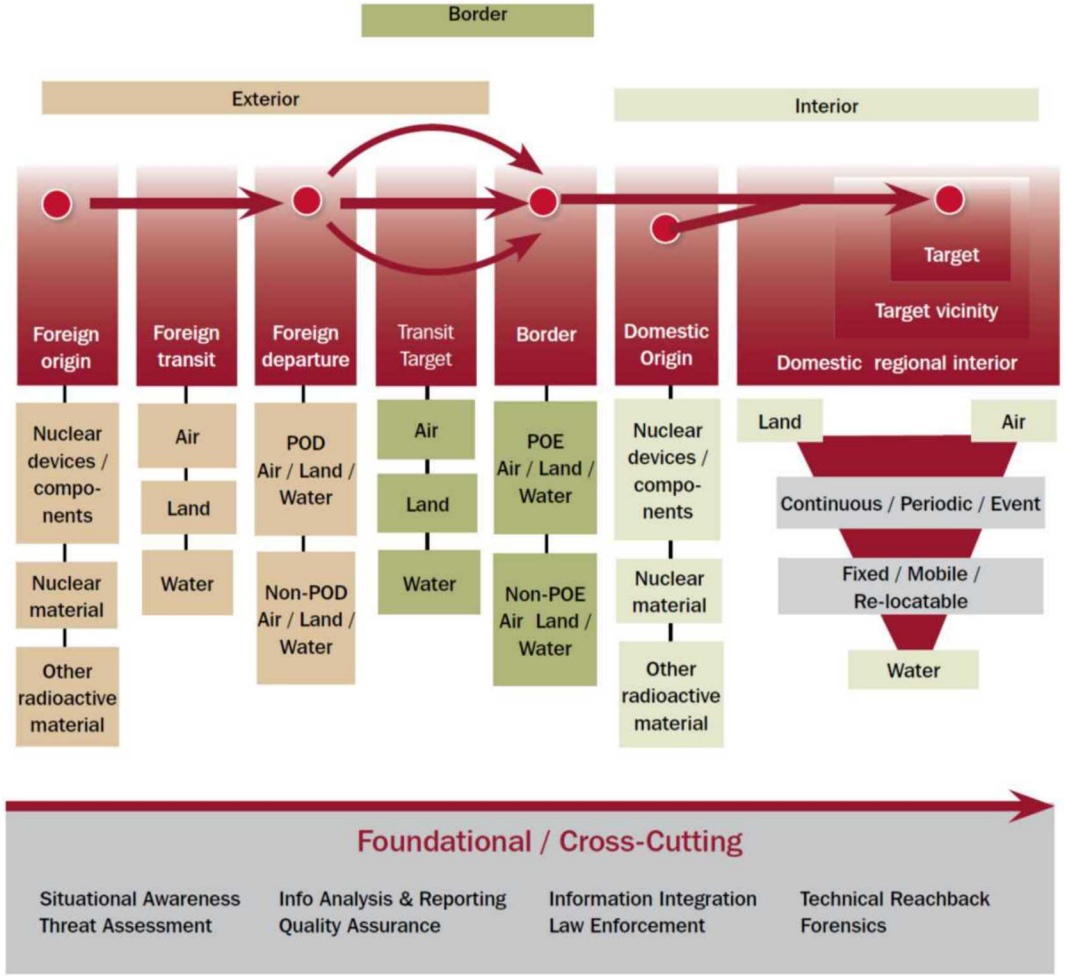

Chemical and biological defense activities – including prevention, detection, and response – can benefit from an "architecture" approach to planning and integration.

What is an architecture?

- An architecture is a conceptual framework that helps stakeholders understand how people, organizations, capabilities, and other assets come together to achieve an overall purpose or strategy
- An architecture is not necessarily intended to override existing organizing concepts, or displace existing capabilities. Rather, it should help users better understand how these existing elements fit together, and help to identify opportunities for optimization and improvement
- Different components or dimensions of an architecture are often illustrated through graphical “operational views” (or “OVs”) that aid communication and dialog. Selection of appropriate views (there are many options) should be driven by intended audiences and communication objectives

Architectures already support U.S. national security in a number of areas.

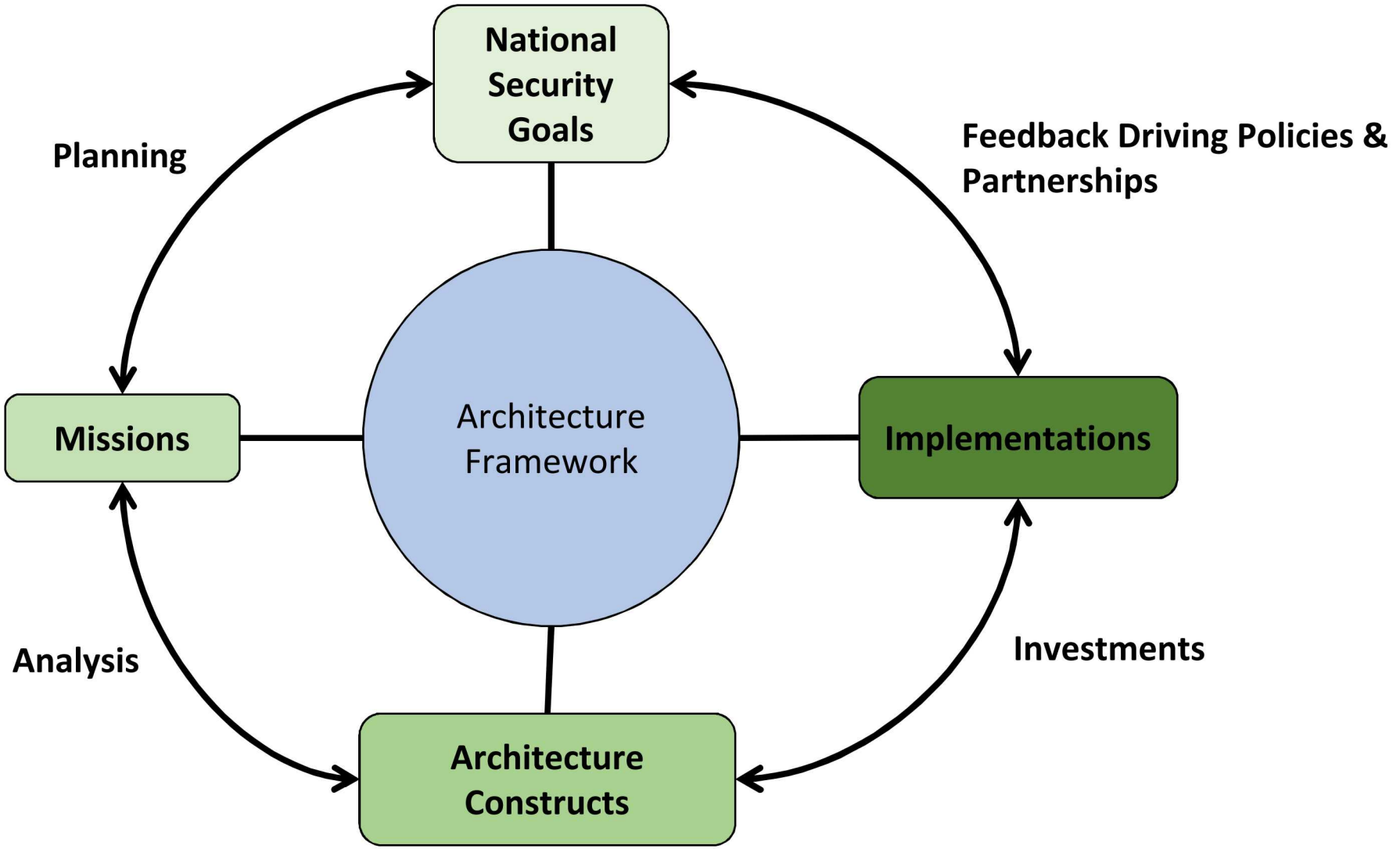
- The Department of Defense Architecture Framework (DODAF) supports planning and system integration for defense programs (and is the conceptual basis for S&T/CBD architecture products)
- The Global Nuclear Detection Architecture (GNDA) is the basis for coordination of U.S. government capabilities for combatting illicit trafficking of nuclear materials; architecture concepts also inform foreign partners in their own implementation
- Sandia has applied architecture concepts to transportation security, CBRN defense, and cyber security, among other areas



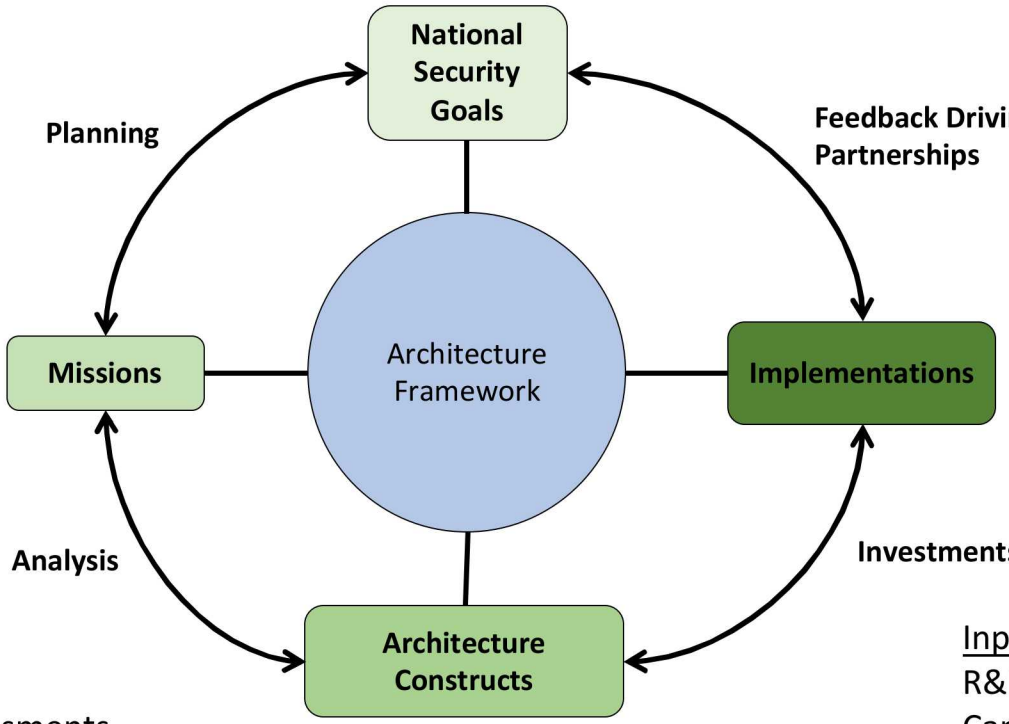
"Pathways" view of a Nuclear Detection Architecture, from the Global Initiative to Combat Nuclear Terrorism *Model Guidelines* document

Proposed architectural framework

- Greater information flow between partners and customers
- Analysis and metrics applied for mission and program determination
- Tracing of program impact to original national security goals



The architecture frames analysis, results, and actionable decisions



Outputs:
Threat awareness
Surveillance
Detection/Diagnostics
Response Recovery

Outputs:
Transitions
Operations
Programs
Plans

These inputs can be satisfied using existing products, such as threat assessments and gap analysis

Inputs:
Budgets
Risk assessments
Requirements
Roles and Responsibilities
Metrics
Trade studies
Models
Current / future options

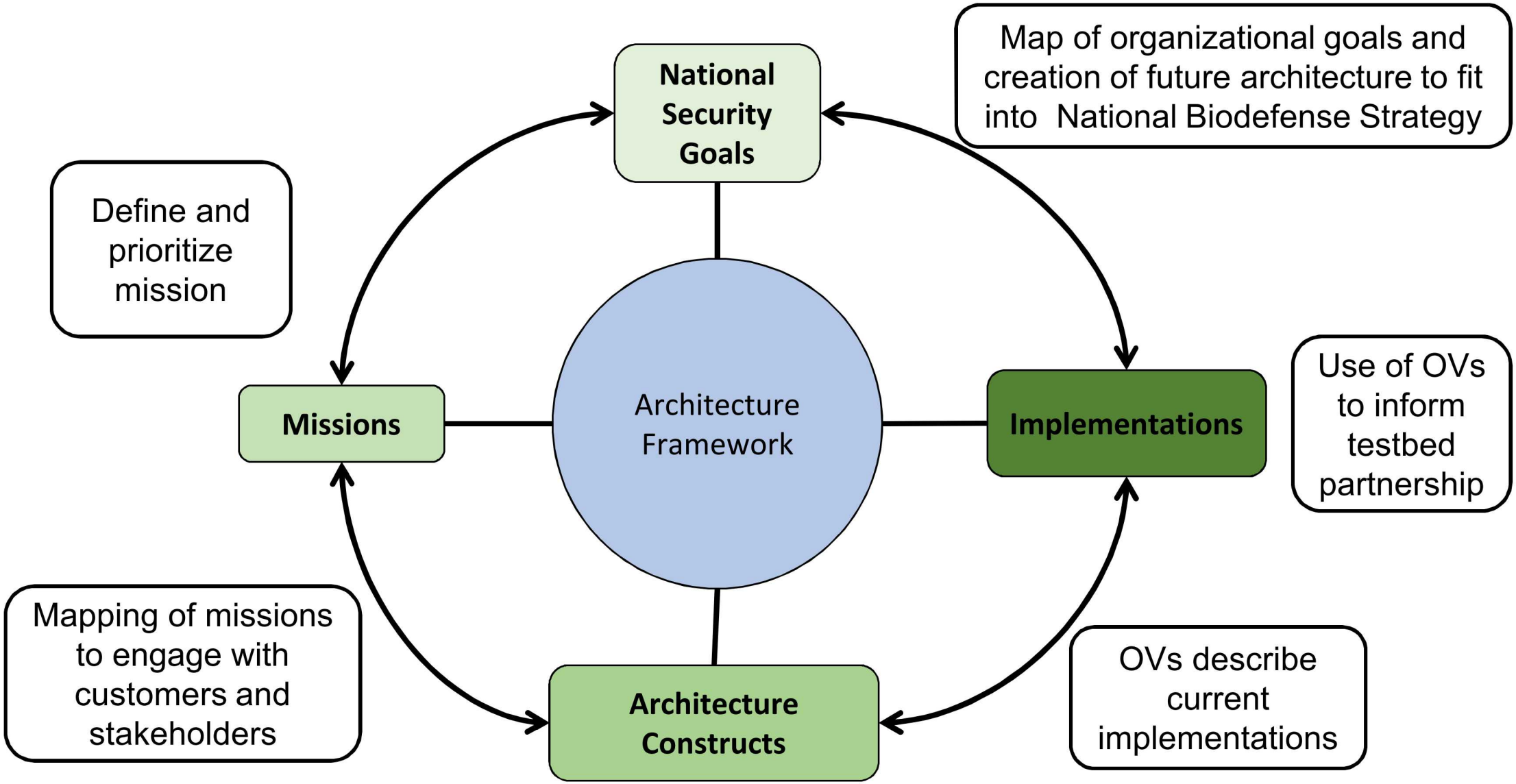
Outputs:
High level Operational Concept
Functional decomposition
Organizational relationships
Activity and Scenario diagrams
Information flow

Inputs:
R&D options
Capability options
- Organizations
- Technology

Optimization metrics

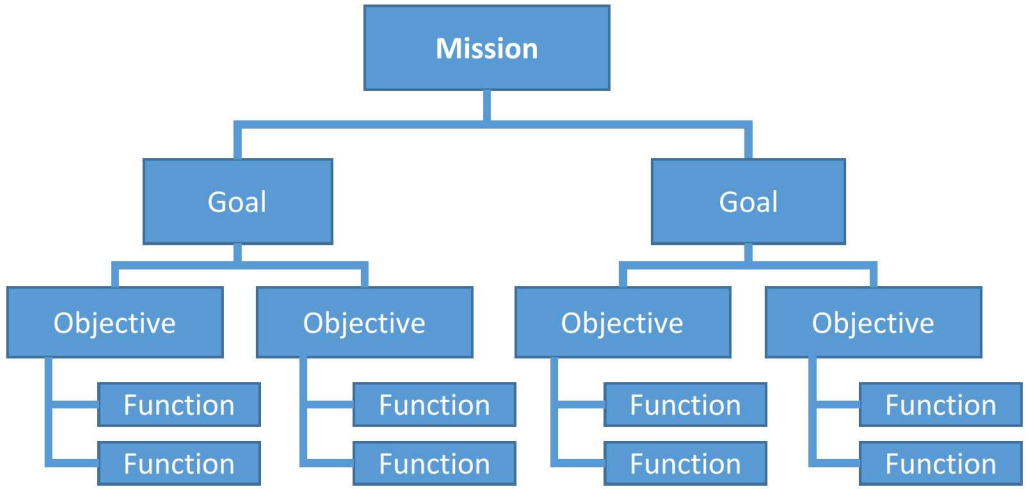
The methodology and analysis enables traceability due to the multidirectional capability

Architectural framework options:



An architecture begins with policy & strategy.

- Policy directives and organizational strategies provide the basis for an architecture, defining the fundamental mission and goals to be achieved
- The architecture development process can be used to derive goals and objectives from policy, if they have not yet been explicitly defined
- It is not uncommon for multiple policies and strategies to coexist; an architecture can help reconcile multiple sources of guidance

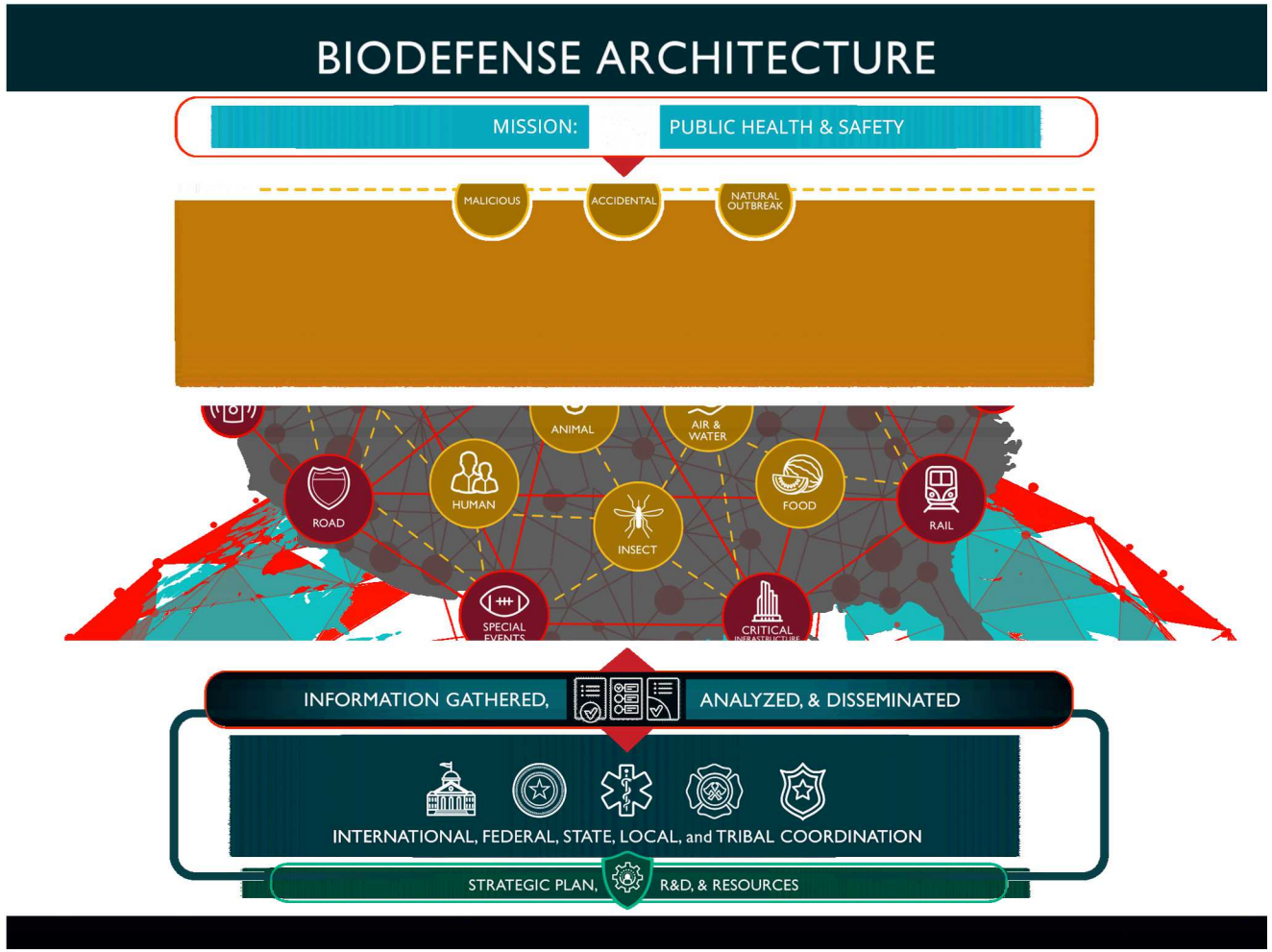


Documents consulted for the S&T CB architecture include:

- *National Biodefense Strategy (2018)*
- *National Response Framework (2016)*
- *S&T Directorate Strategic Plan (2015)*
- *BioWatch Preparedness & Response Guidance*

At the highest level, an architecture helps define a common operating picture.

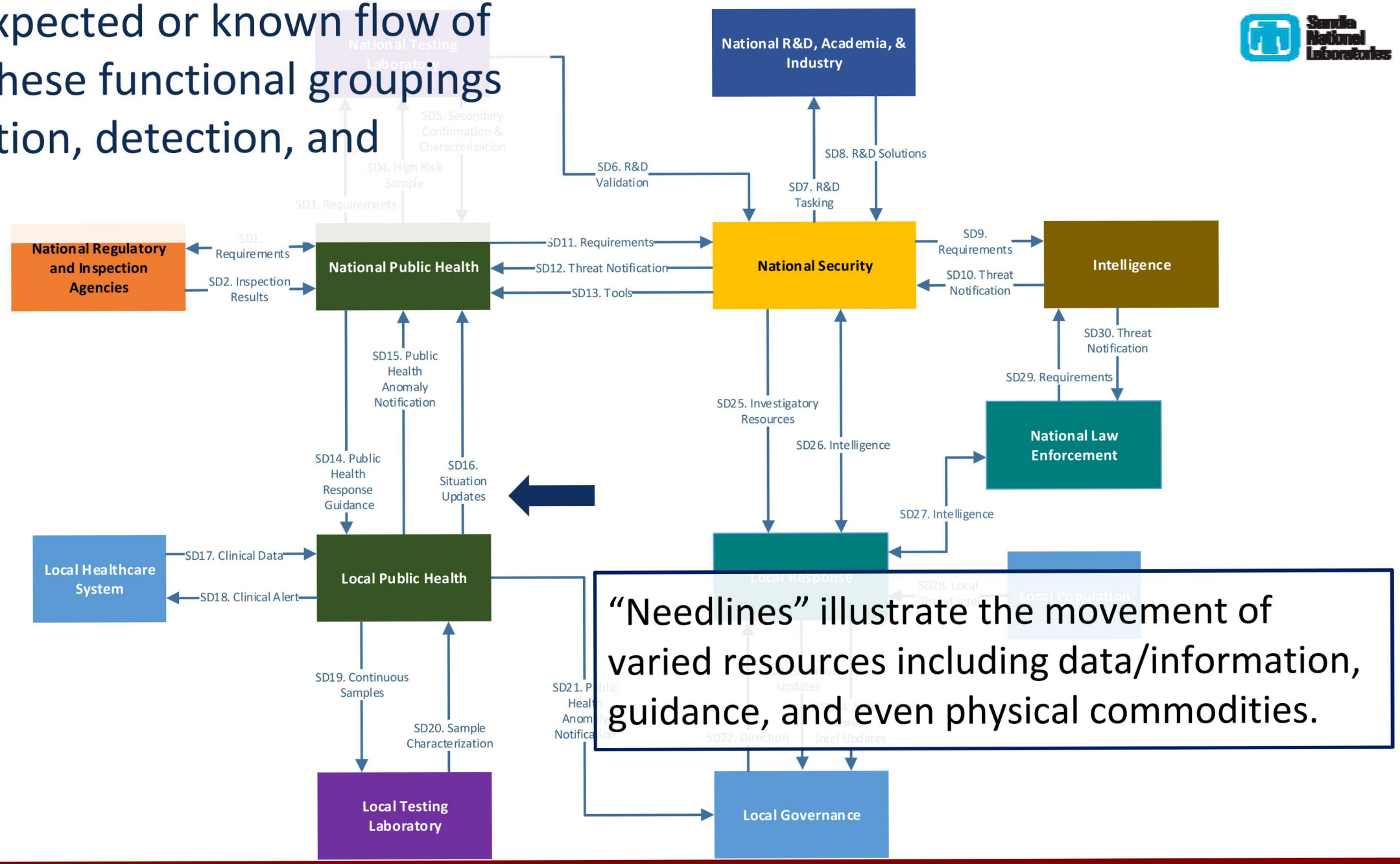
- The High Level Operational Concept view (or OV1) communicates mission and key elements of a chem-bio defense strategy
- The visual narrative will vary with different stakeholder communication requirements. Common OV1 elements include:
  - A statement of purpose or mission
  - Definition of the threat/hazard
  - Identification of key defensive or operational priorities
  - Visual and textual explanation of how these elements interact operationally
- **As visual impact is critical for an OV1, graphic designers should be included from the beginning of development**



Subsequent OVs provide more detailed insight into different functional dimensions of the architecture.

- The Operational Resource Flow view (OV2) begins with broadly defined functional roles in the architecture
- These roles might be derived from strategy documents, or represent a consensus among architecture stakeholders
- Depending on the scope of the architecture, or specific questions that need to be addressed, there may be value in separating state, local, tribal, and federal functional roles

maps the expected or known flow of
s between these functional groupings
n to prevention, detection, and
activities.



"Needlines" illustrate the movement of varied resources including data/information, guidance, and even physical commodities.

A corresponding Operational Resource Flow Matrix (OV3) adds further detail and supports analysis.

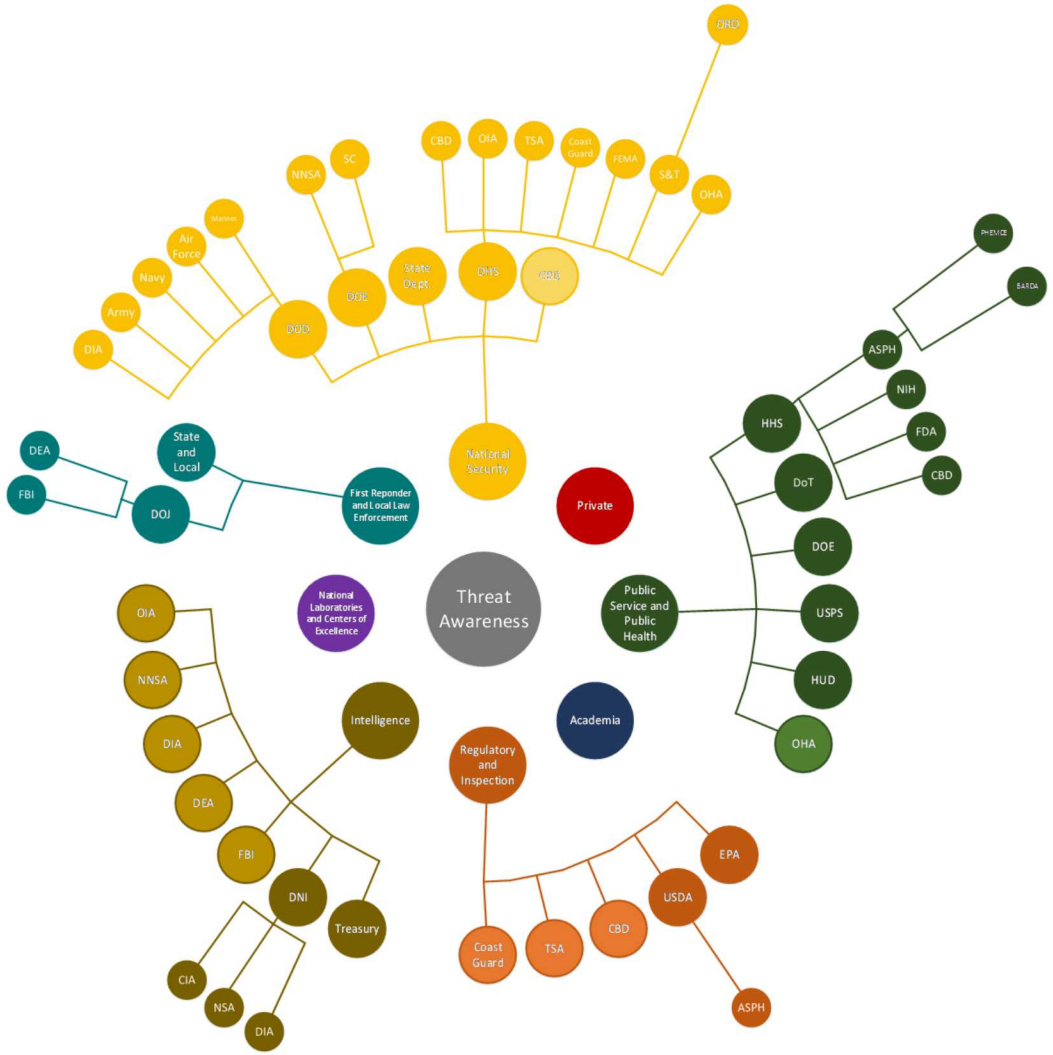
- The OV3 provides additional descriptive detail for OV2 needlines
- Source material for the matrix can include planning documents and dialog with stakeholders
- In addition to sender/receiver and activity information, users might also include requirements for:
  - Quality
  - Timeliness
  - Interoperability
  - Classification/sensitivity

Need-line #	Needline Name	Detailed Resource Description	Sending Node	Receiving Node	Sending Node Operational Activity	Receiving Node Operational Activity
SD1	Requirements	Requirements for monitoring and reporting	National Public Health	National Regulatory and Inspection Agency	Set and communicate requirements	Implement requirements through regulatory inspection process
SD2	Inspection Results	Results from inspection of regulated entities	National Regulatory and Inspection Agency	National Public Health	Carry out inspection & communicate results	Receive results and monitor compliance
SD3	Requirements	Capability requirements for pathogen identification, characterization, & reporting	National Public Health	National Testing Laboratory	Set and communicate requirements	Receive requirements and develop concurrent capabilities
SD4	High Risk Sample	Sample of potential high risk pathogen	National Public Health	National Testing Laboratory	Collect and deliver sample	Receive sample and conduct analysis, identification, and characterization
SD5	Secondary Confirmation & Characterization	Confirm/disconfirm pathogen identity and characterize	National Testing Laboratory	National Public Health	Communicate analysis results	Receive results and use to inform decision making
SD6	R&D Validation	Validation of surveillance & detection technologies and techniques	National Testing Laboratory	National Security	Formulate and communicate RFPs and tasking	Receive RFPs and tasking and develop project proposals and plans
SD7	R&D Tasking	RFPs and tasking for bio surveillance & detection R&D	National Security	National R&D, Academia, & Industry	Formulate and communicate RFPs and tasking	Receive RFPs and tasking and develop project proposals and plans
SD8	R&D Solutions	Technology and analytical products supporting bio surveillance and detection	National R&D, Academia, & Industry	National Security	Develop, test & evaluate, and deliver R&D solutions	Evaluate and accept/reject R&D solutions for deployment

Organizational Relationship views (OV4) help clarify functional relationships between stakeholders.

- Like the OV2, an OV4 begins with functional groupings
- These groupings are then decomposed into further subgroupings and/or constituent agencies at the federal, state, tribal, or local level
- Agencies can be further decomposed into constituent offices, and even programs as appropriate
- Secondary relationships that exist across functional groupings can also be highlighted

OV4 mapping can help clarify functional lanes, highlight complementary roles, & identify partnership opportunities.

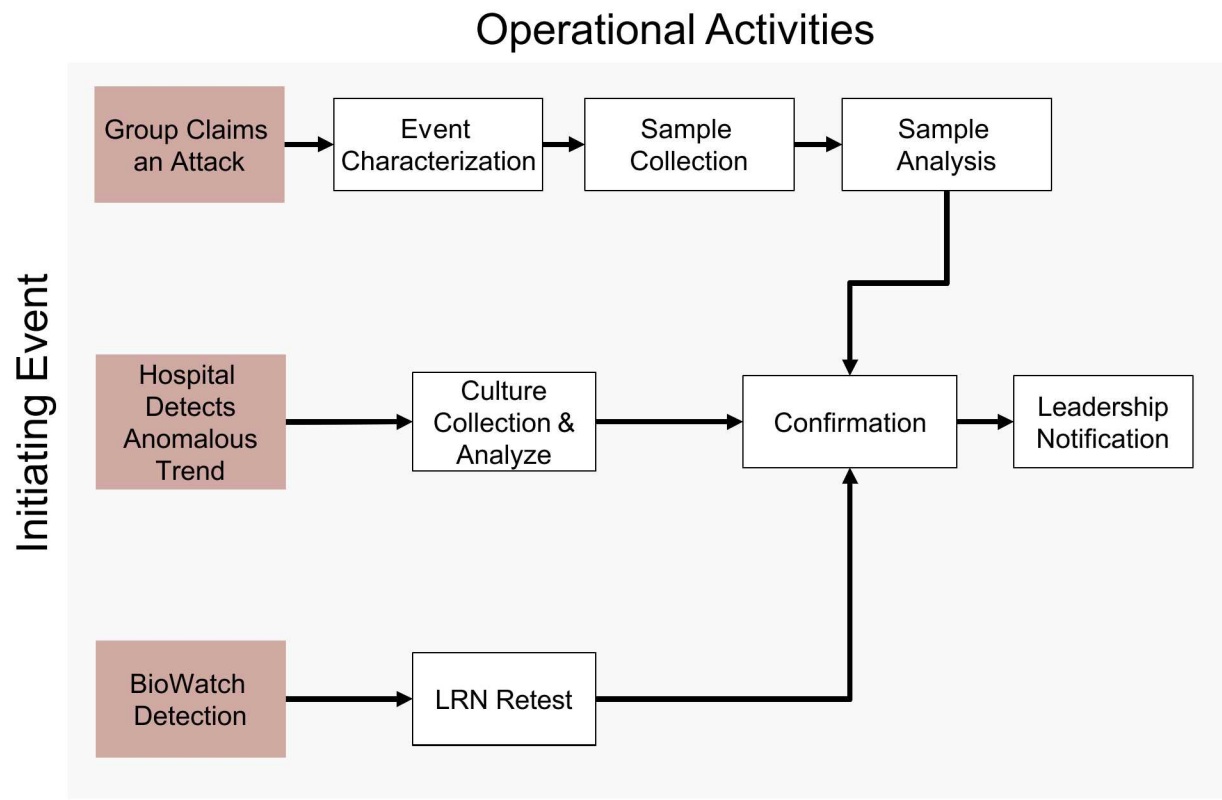


- Functional relationships may be broader in scope or more interconnected than some stakeholders realize
- The OV4 provides a starting point for interagency conversations on each stakeholder's place and role in the overall architecture

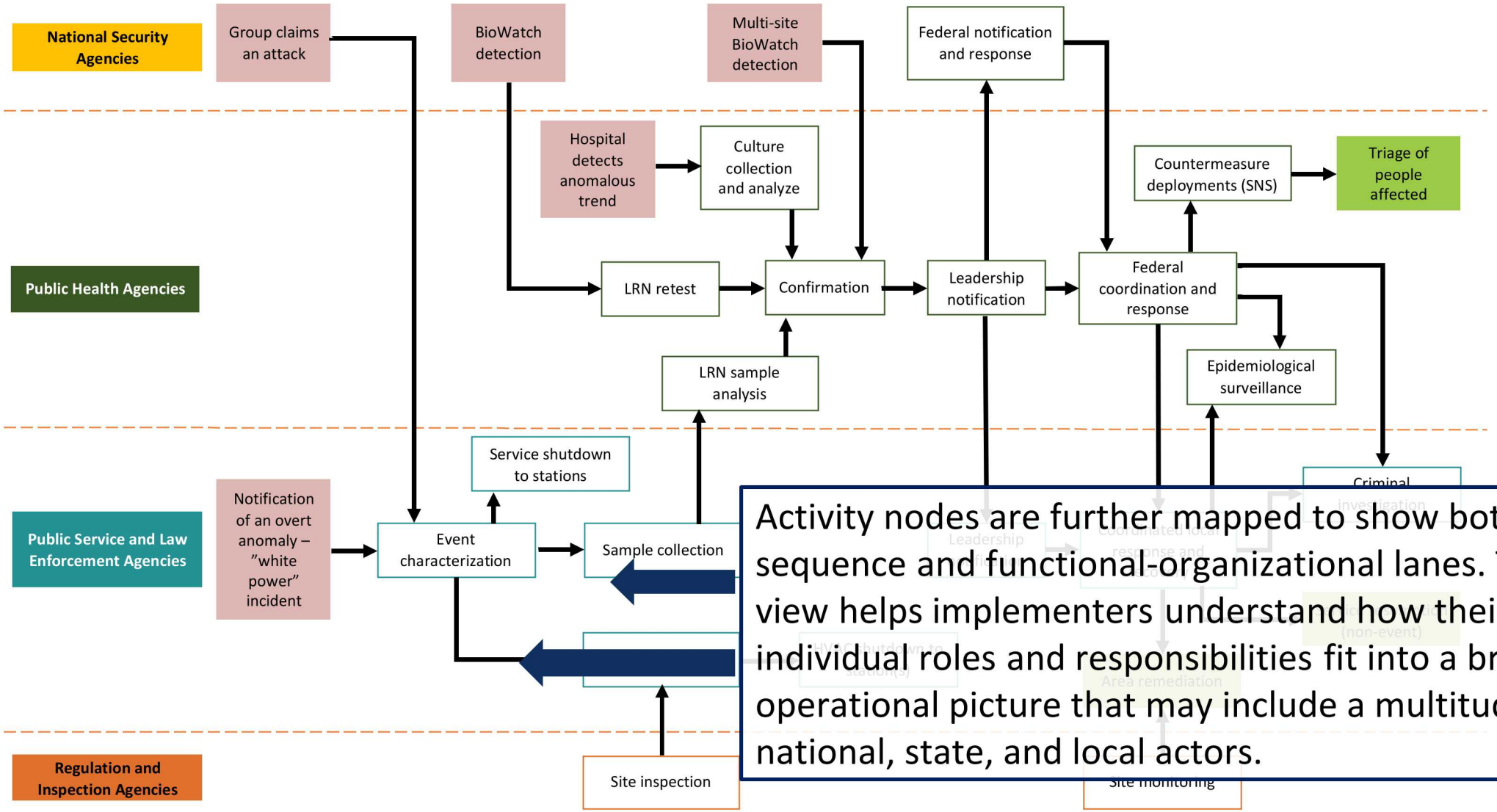
Operational roles & responsibilities may vary depending on incident type.

- An Operational Activity Decomposition (OV5) details the sequence of activities undertaken by stakeholders in a given operational context
- Development begins with selection of an operational scenario (e.g. an assumed combination of threat and target in prevention, detection, and/or response phase)
- The sequence of activities is first mapped, drawing upon documented concepts of operations (CONOPs) and stakeholder consultation

Scenario: Urban Underground Transportation Biological Agent Release (Detection Phase)



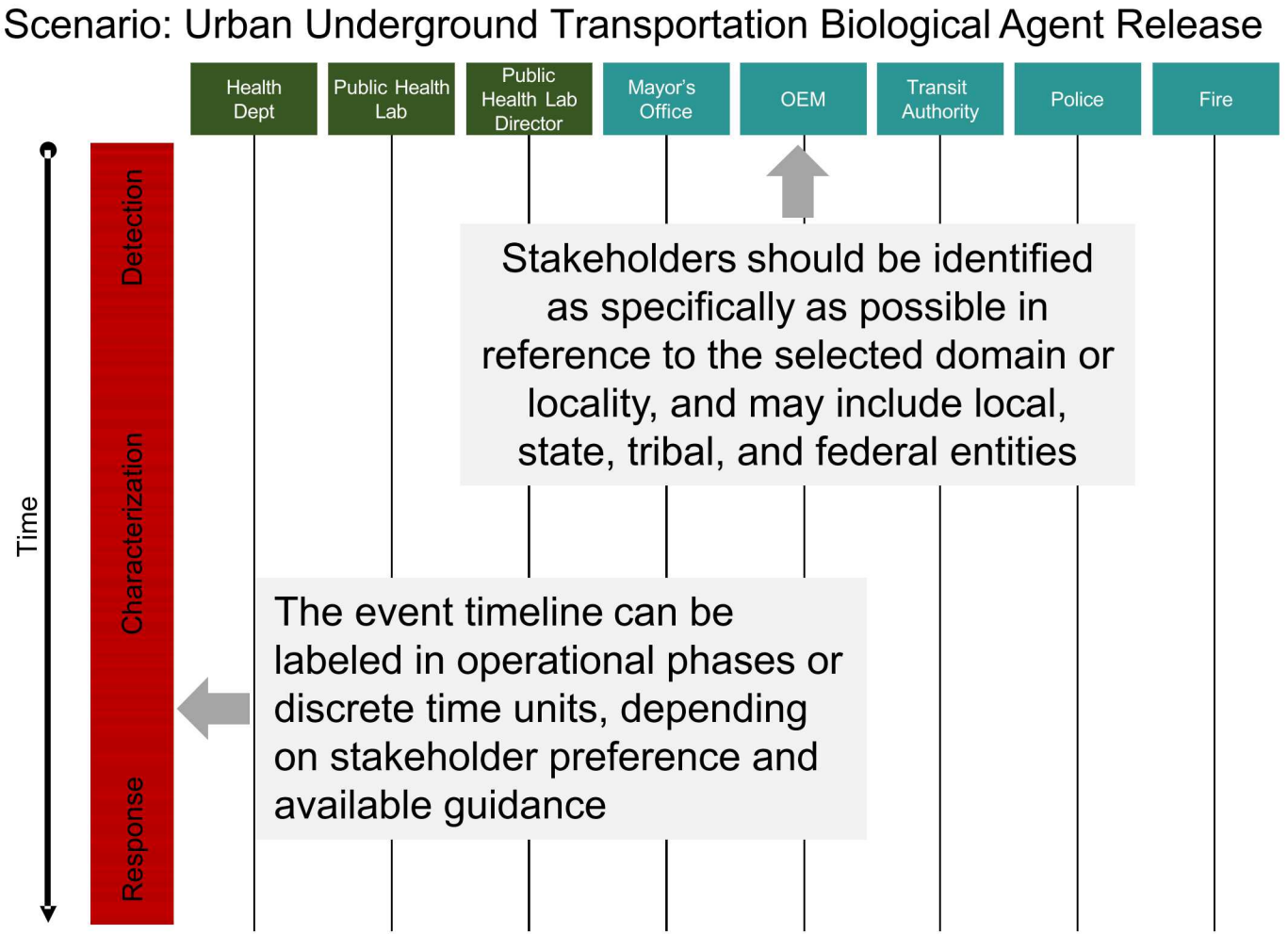
OV5: Urban Underground Transportation Biological Agent Release, Detection Phase



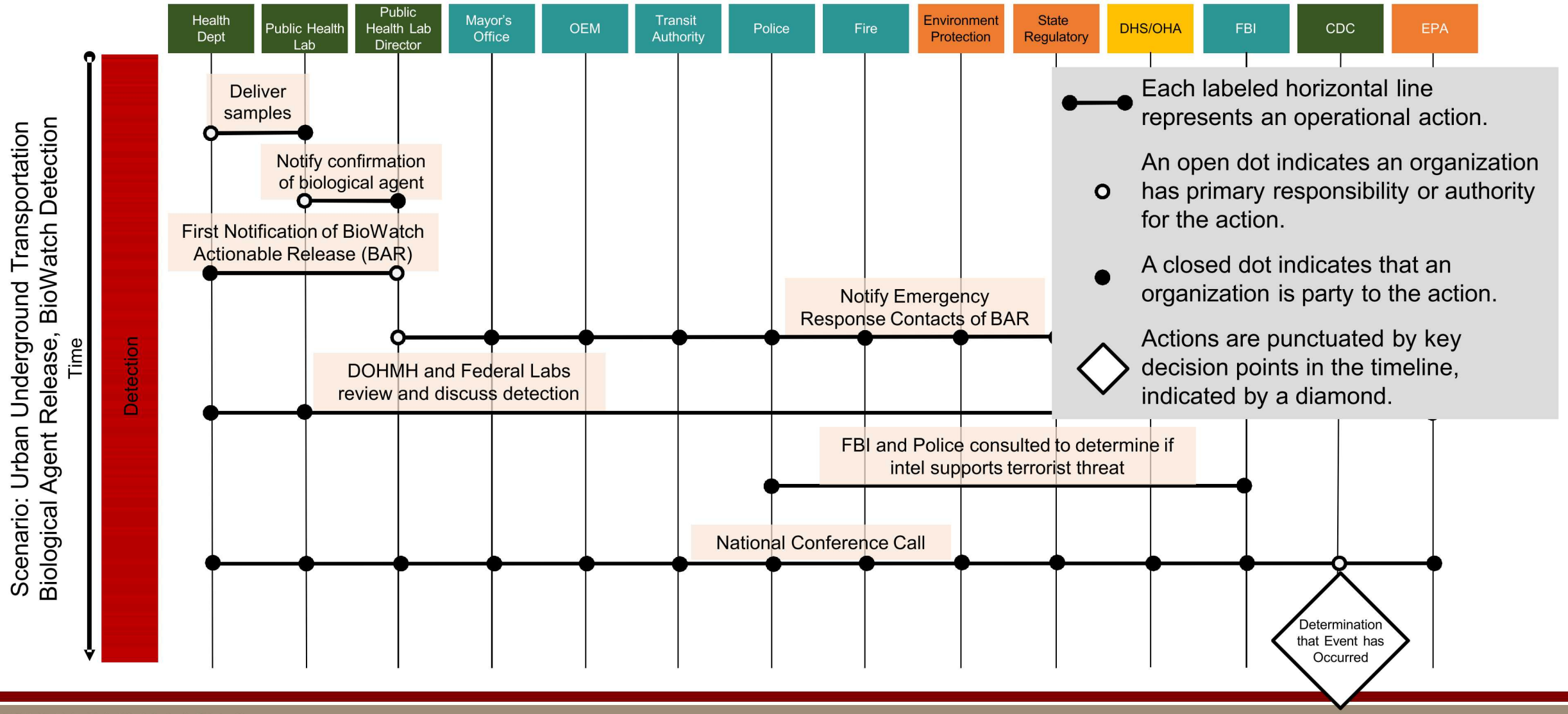
Activity nodes are further mapped to show both sequence and functional-organizational lanes. This view helps implementers understand how their individual roles and responsibilities fit into a broader operational picture that may include a multitude of national, state, and local actors.

More detail may be required to understand decision processes in specific operational circumstances.

- An Operational Event-trace (OV6) provides additional detail regarding time, sequence, and the functions of specific stakeholder organizations
- Development begins with identification of a scenario situated within a real-world operational locality

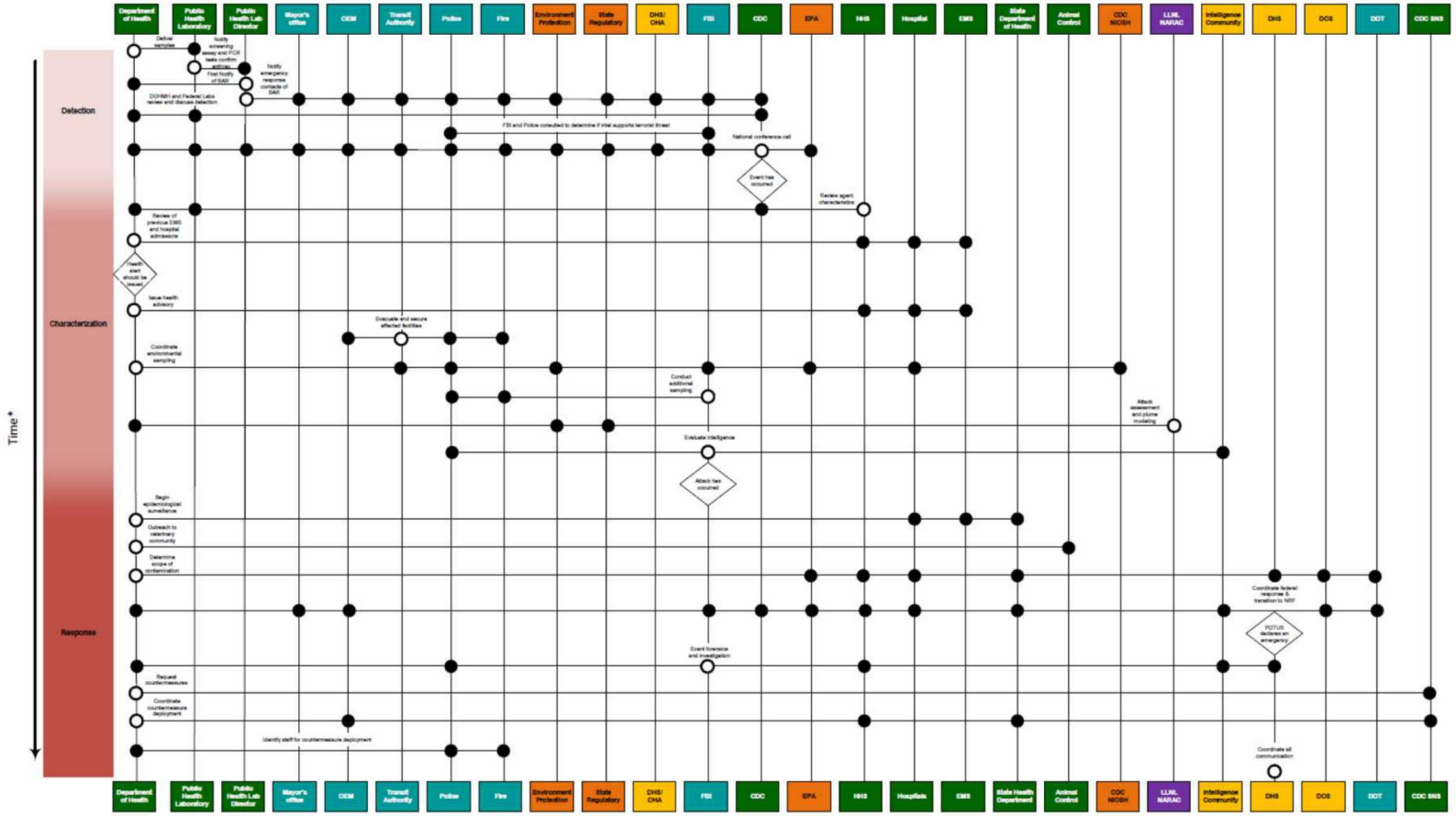


The OV6 provides a clearer sense of how actions and decisions map to specific organizations over time.

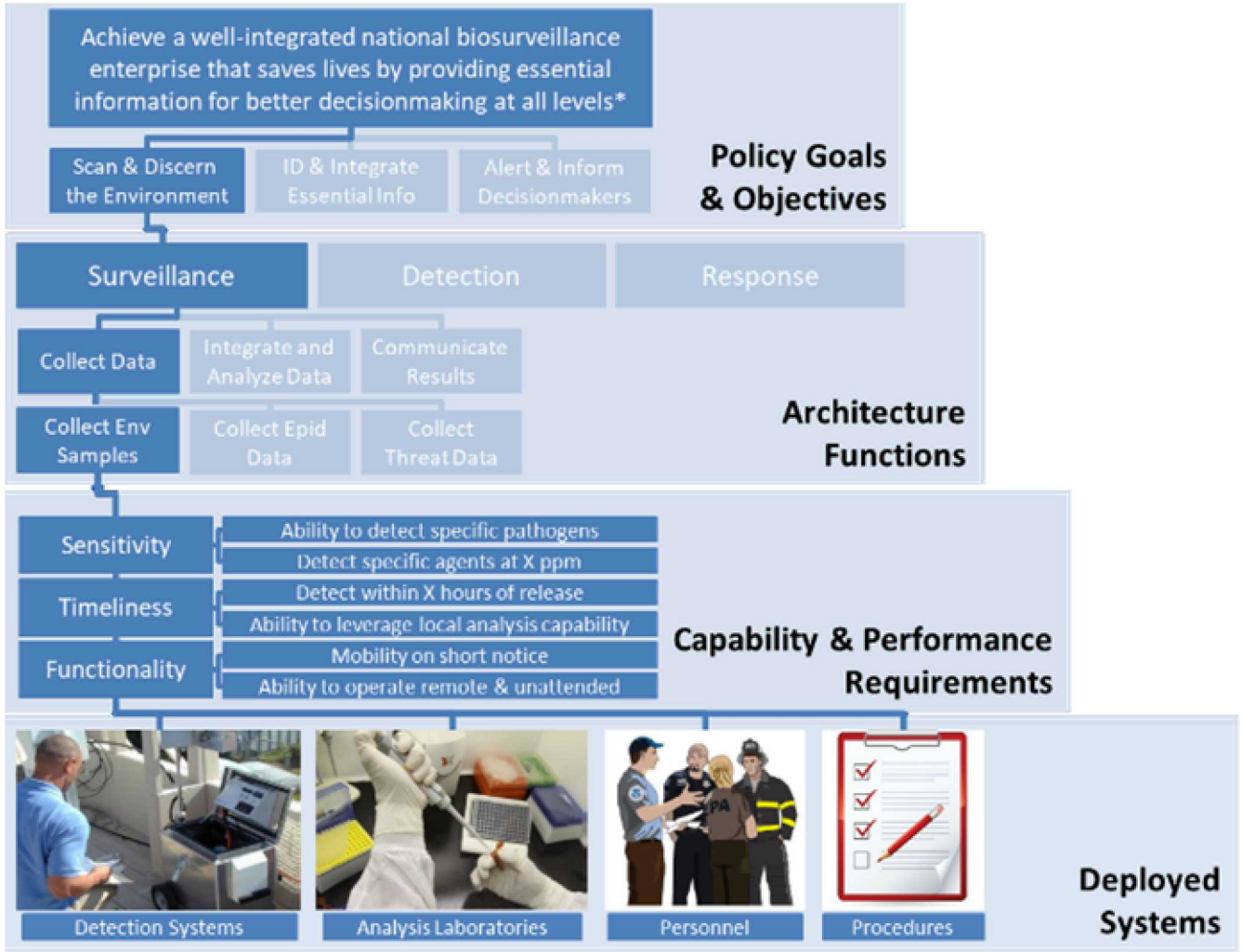


The OV6 supports both communication and analysis.

- Planning documents and stakeholder consultation provide the detailed information required for an OV6; this creates opportunity for engagement and development of shared understandings
- The OV6 also supports identification of procedural inconsistencies, bottlenecks, gaps, and overlaps – information that can be used to support process optimization



An architecture facilitates more systematic and efficient definition of capability requirements and priorities.



- By understanding their role within a larger architecture, implementers can better define requirements that meet strategic and operational needs, minimize redundancies, and integrate with partner capabilities
- The architecture can be also be used to make a more compelling case for assistance in acquisition and development of requisite capabilities

There is no “one size fits all” template for an architecture; development is an iterative and consultative process.

- Every organization faces unique challenges and implementing contexts; these details should be reflected in the various architecture products
- Development should involve a conversation among relevant stakeholders, to ensure that perspectives and interests are accurately represented
- The assumptions and organizing principles behind an architecture should be periodically revisited in light of evolving threats, technology developments, new policies, or other changes in the implementing environment

POTENTIAL NEXT STEPS

Analysis Options

- Data captured through the OV development process can be leveraged in support of multiple analysis directions:
  - Functional analysis
  - Capability mapping & gap analysis
  - Program portfolio analysis
  - Optimization analysis
  - Decision support analysis
- Analysis can provide both **technical** and **operational** options

Capability Mapping & Gap Analysis

- The OV2 and OV3 are derived from existing documentation and suggest that certain capabilities *should* exist in support of needlines:
  - Communication networks
  - Concepts of Operation
  - Data collection and analysis capabilities
  - Trained personnel
- We know that operational implementation often differs from documented plans
- A capabilities mapping and gap analysis would include:
  1. Identifying specific technical and non-technical capabilities associated with OV2/OV3 needlines
  2. Conducting an inventory of existing capabilities through partner and end-user outreach
  3. Identifying gaps or inconsistencies relative to our conceptualization of the architecture
  4. Analyzing gaps to identify systematic issues and trends
  5. Develop recommendations for addressing gaps and/or further reconceptualizing the architecture

Sample Qualitative Evaluation of Capabilities: Notional Data

Need-line #	Needline Name	Detailed Resource Description	Sending Node	Receiving Node	Timeliness Requirement	Interoperability Requirement	Sensitivity/ Classification	Quality
SD1	Requirements	Requirements for monitoring and reporting	National Public Health	National Regulatory and Inspection Agency				
SD2	Inspection Results	Results from inspection of regulated entities	National Regulatory and Inspection Agency	National Public Health				
SD3	Requirements	Capability requirements for pathogen identification, characterization, & reporting	National Public Health	National Testing Laboratory				
SD4	High Risk Sample	Sample of potential high risk pathogen	National Public Health	National Testing Laboratory				
SD5	Secondary Confirmation & Characterization	Confirm/disconfirm pathogen identity and characterize	National Testing Laboratory	National Public Health				
SD6	R&D Validation	Validation of surveillance & detection technologies and techniques delivered by National R&D to National Security	National Testing Laboratory	National Security				
SD7	R&D Tasking	RFPs and tasking for bio surveillance & detection R&D	National Security	National R&D, Academia, & Industry				
SD8	R&D Solutions	Technology and analytical products supporting bio surveillance and detection	National R&D, Academia, & Industry	National Security				
SD9	Requirements	Requirements for notification and reporting of bio threats to the US and interests abroad	National Security	Intelligence				
SD10	Threat Notification	Notification of current and emerging bio threats to the US and interests abroad	Intelligence	National Security				
SD11	Requirements	Requirements for threat notification & tools supporting surveillance & detection	National Public Health	National Security				
SD12	Threat Notification	Notification of current or emerging bio threats	National Security	National Public Health				

Qualitative evaluation of capabilities can drive engagement and provide a method for prioritization

Capability Mapping & Gap Analysis

Need-line #	Needline Name	Detailed Resource Description	Sending Node	Receiving Node	Sending Node Operational Activity	Receiving Node Operational Activity	Capability Requirement	Capability Inventory
SD18	Clinical Alert	Notification of potential bio threats and reporting requirements	Local Public Health	Local Healthcare System	Communicate notification	Receive notification and inform clinicians	• Designated points of contact • Notification protocol	• POCs identified and documented • Formal notification protocol does not exist
SD19	Continuous Samples	Samples collected from continuous bio surveillance stations	Local Public Health	Local Testing Laboratory	Collect and deliver samples	Receive and analyze samples	• Sample collection stations • Trained personnel • Collection & delivery protocol	• BioWatch stations deployed at strategic locations and special events • Local public health authority personnel assigned to collection and delivery • Protocol developed in consultation with DHS
SD20	Sample Characterization	Characterization of potential bio threat pathogen samples	Local Testing Laboratory	Local Public Health	Communicate analysis results	Receive analysis results and use to inform decision making and guidance	• Laboratory analysis capability • Trained personnel • Communication protocol	• Designated testing laboratory operated by local public health authority • Laboratory personnel trained to conduct analysis and characterization • Laboratory personnel overtasked and often deprioritize sample analysis • Formal communication protocol does not exist

Program Portfolio Analysis

- A portfolio analysis would build on the capability mapping and gap analysis by:
  - Identifying where existing S&T programs map to the architecture as described in the OV2 & OV3
  - Demonstrating how S&T programs address known architecture gaps, or where known gaps lack programmatic covering
  - Supporting future prioritization and portfolio balancing

Need-line #	Needline Name	Detailed Resource Description	Sending Node	Receiving Node	Capability Requirement	Capability Inventory	S&T Program Support
SD18	Clinical Alert	Notification of potential bio threats and reporting requirements	Local Public Health	Local Healthcare System	• Designated points of contact • Notification protocol	• POCs identified and documented • Formal notification protocol does not exist	State and local outreach programs addressing protocol development
SD19	Continuous Samples	Samples collected from continuous bio surveillance stations	Local Public Health	Local Testing Laboratory	• Sample collection stations • Trained personnel • Collection & delivery protocol	• Environmental detection stations deployed at strategic locations and special events • Local public health authority personnel assigned to collection and delivery • Protocol developed in consultation with DHS	Ongoing environmental detection program support, including: • System maintenance • Training & exercise support • Next generation R&D
SD20	Sample Characterization	Characterization of potential bio threat pathogen samples	Local Testing Laboratory	Local Public Health	• Laboratory analysis capability • Trained personnel • Communication protocol	• Designated testing laboratory operated by local public health authority • Laboratory personnel trained to conduct analysis and characterization • Laboratory personnel overtasked and often deprioritize sample analysis • Formal communication protocol does not exist	None currently. Recommended future program development includes: • Awareness-building outreach to analysis laboratory • Assistance in development of more streamlined laboratory testing procedure • Possible resource assistance • State and local outreach on protocol development

Optimization Analysis

- Parameters or metrics can be specified for the OV2 and OV3 needlines. Examples might include:
  - Time requirements
  - Interoperability requirements
  - Data quality/integrity
  - Information security
- Optimization analysis would include:
  1. Specifying program-relevant parameters/metrics and identifying targets or requirements
  2. Conducting analysis of how these parameters might be balanced in a hypothetically optimized system
  3. Gathering data, in consultation with partners, on current system performance
  4. Conducting analysis of how the current system performs relative to targets or requirements
  5. Identifying system failure points or bottlenecks and associated recommendations for achieving system optimization

Optimized Architecture

Need-line #	Needline Name	Detailed Resource Description	Send Node	Receive Node	Sending Node Operational Activity	Receiving Node Operational Activity	Time Requirement	Interoperability Requirement	Data Quality/ Integrity	Information Security
SD18	Clinical Alert	Notification of potential bio threats and reporting requirements	Local Public Health	Local Healthcare System	Communicate notification	Receive notification and inform clinicians	Notification within 4-6 hours of identification of confirmed threat	None	Minimal Requirement	FOUO-level protection protocols (minimal delay)
SD19	Continuous Samples	Samples collected from continuous bio surveillance stations	Local Public Health	Local Testing Laboratory	Collect and deliver samples	Receive and analyze samples	Retrieval and delivery of samples once every 24 hours	Laboratory testing capabilities should be compatible with sample format	throughout transfer process	Continuous chain of custody in sample handling
SD20	Sample Character-ization	Characterization of potential bio threat pathogen samples	Local Testing Laboratory	Local Public Health	Communicate analysis results	Receive analysis results and use to inform decision making and guidance	Analysis and characterization within 24 hours of sample receipt	None	Characterization must accurately represent testing results and support timely decision making	FOUO-level protection protocols (minimal delay)

Possible Impact on Information Security and Delivery Timelines

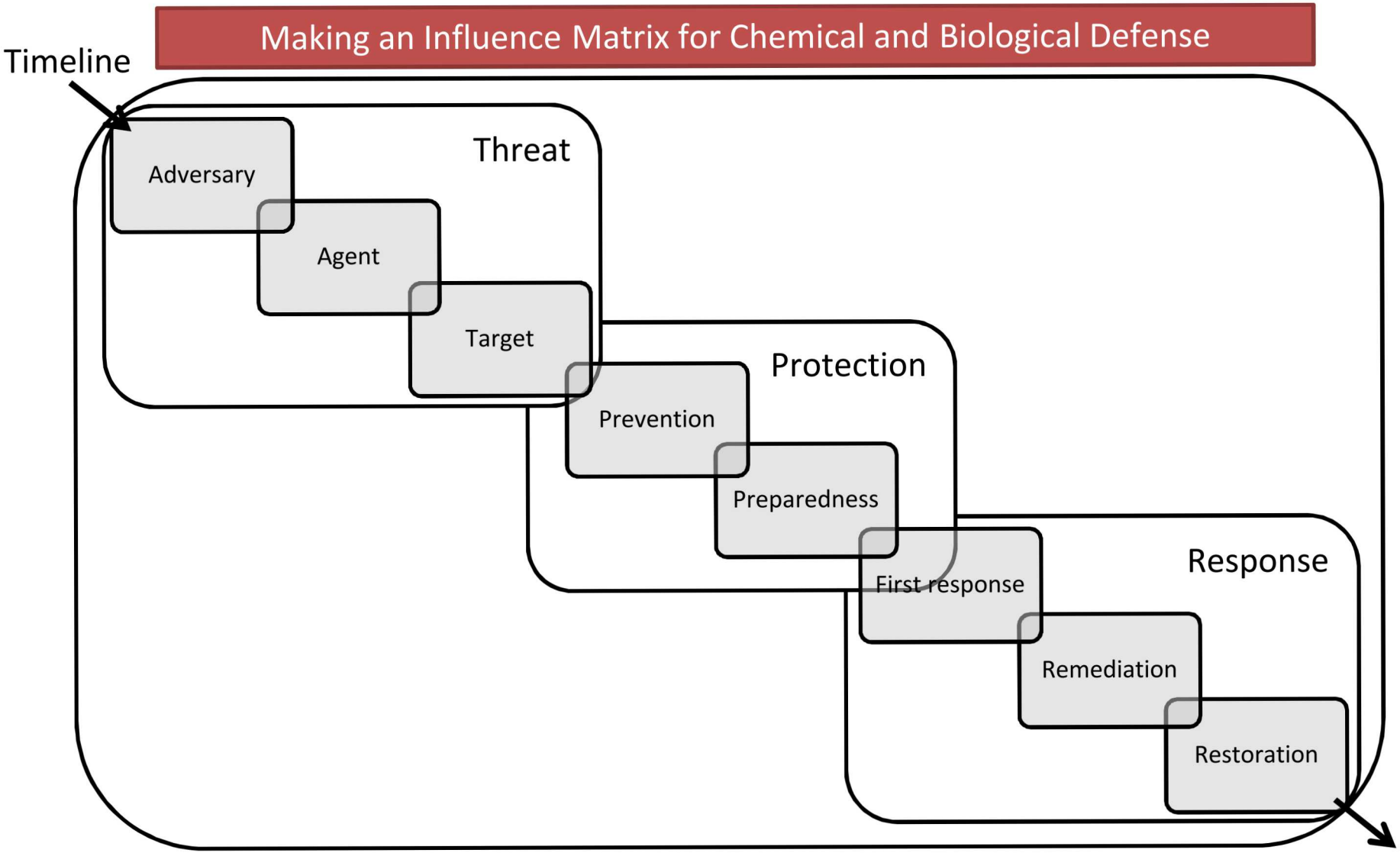
Existing Architecture

Need-line #	Needline Name	Detailed Resource Description	Send Node	Receive Node	Sending Node Operational Activity	Receiving Node Operational Activity	Time Requirement	Interoperability	Data Quality/ Integrity	Information Security
SD18	Clinical Alert	Notification of potential bio threats and reporting requirements	Local Public Health	Local Healthcare System	Communicate notification	Receive notification and inform clinicians	Notification within 5 hours of identification of confirmed threat		Minimal Requirement	FOUO-level protection protocols (minimal delay)
SD19	Continuous Samples	Samples collected from continuous bio surveillance stations	Local Public Health	Local Testing Laboratory	Collect and deliver samples	Receive and analyze samples	Retrieval and delivery of samples once every 24 hours	Laboratory testing capabilities compatible with sample format	Sample integrity maintained throughout transfer process	Continuous chain of custody requirements not formalized
SD20	Sample Character-ization	Characterization of potential bio threat pathogen samples	Local Testing Laboratory	Local Public Health	Communicate analysis results	Receive analysis results and use to inform decision making and guidance	Analysis and characterization generally processed in 36-48 hours	None	Characterization results delivered in raw data format, requiring SME interpretation	FOUO-level protection protocols (minimal delay)

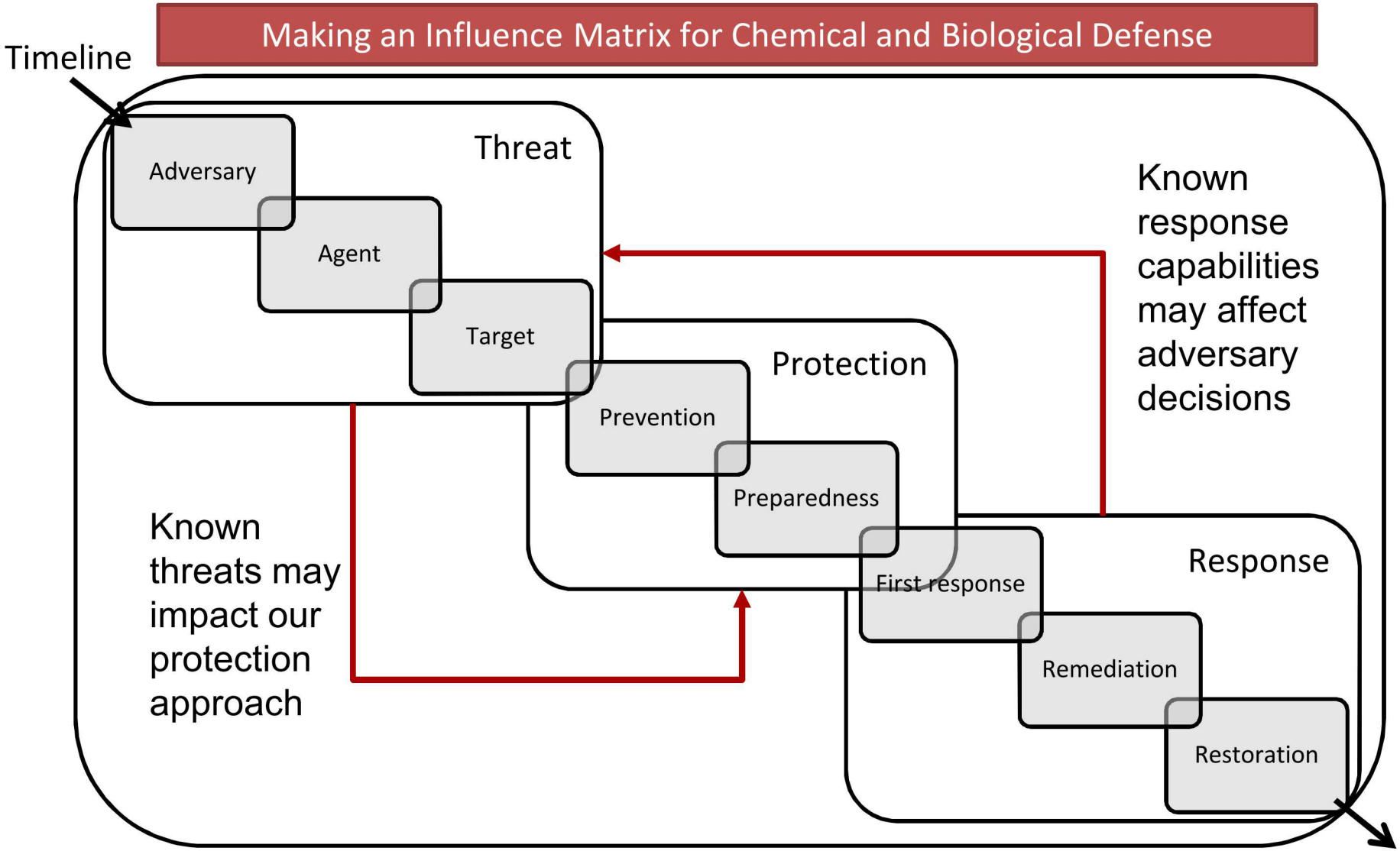
Significant Impact on Decision & Response Timeline

MAPPING RISK ASSESSMENTS TO THE ARCHITECTURE

Mapping Risks to the Architecture



Mapping Risks to the Architecture



Mapping Risks to the Architecture

Making an Influence Matrix for Chemical and Biological Defense

Timeline

Threat

Adversary

Agent

Target

Protection

Prevention

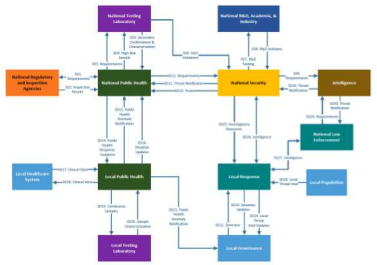
Preparedness

Response

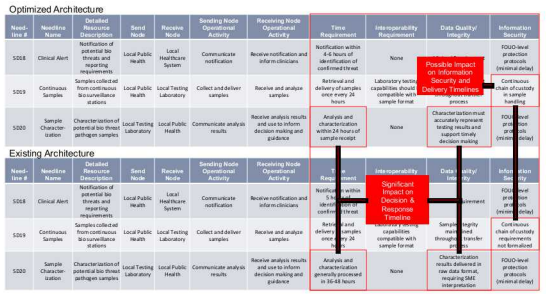
First response

Remediation

Restoration



Timeliness Requirement	Interoperability Requirement	Sensitivity/ Classification	Quality



Mapping risks allows tracing of analysis products and new programs to determine overall benefit to the architecture

Conclusions & Next Steps

- The architecture allows for multiple analysis products to determine gaps and priorities for addressing them
- While the architecture may also be used to determine requirements, it can also act as a quality control measure to ensure the full end-to-end engagement
- Understanding how risks can be directly mapped to each component of the architecture enables greater tracing of impact