SANDIA REPORT
SAND2019-14727
Printed March 2019

Sandia National Laboratories

DHS Chemical and Biological Defense Architecture Development

Ben Bonin[1], Nataly Beck[2], Patricia Hernandez[1], Trisha Miller[1], Janson Wu[1]

[1]*Systems Research & Analysis*
[2]*Biotechnology & Bioengineering*
Sandia National Laboratories
Livermore, CA

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

This report describes application of architecture concepts to the chemical-biological defense space, as requested by the Chemical & Biological Defense (CBD) Program at the Science and Technology Office, U.S. Department of Homeland Security, for purposes of 1) understanding and characterizing system interdependencies and 2) prioritizing program development and allocation of resources. A series of graphical Operational Views (OVs) are presented, characterizing a notional chem-bio architecture at increasing levels of detail. Development best practices are highlighted, as well as potential analytical applications.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
CBD	Chemical and Biological Defense Department
CONOPS	Concept of Operations
DHS	Department of Homeland Security
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
OV	Operational view
S&T	Science and Technology

1. ARCHITECTURE CONCEPT OVERVIEW

The content in this report was developed in response to a request from the former Chemical & Biological Defense (CBD) Program at the Science and Technology (S&T) Office, Department of Homeland Security (DHS). CBD was responsible for increasing the nation's preparedness against chemical and biological threats through improved threat awareness, advanced surveillance and detection, and responsive countermeasures. The program worked with industry, academic, national laboratory and federal partners to develop technologies, systems, and knowledge products to increase national preparedness.[1]

CBD tasked Sandia National Laboratories to develop an architecture that describes the chemical and biological defense space in order to 1) understand and characterize system interdependencies and 2) prioritize program development and allocation of resources. The intended audiences for this product potentially include DHS senior leaders and program leads, members of congress, and state and local partners.

1.1. Architectures

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) formally define an architecture, in the context of systems and software engineering, as:

> "Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution."[2]

Outside software engineering, an architecture can be more pragmatically and simply described as a conceptual framework that helps stakeholders understand how people, organizations, capabilities, and other assets come together to achieve an overall purpose or strategy. The idea of an architecture is not new; it is a concept employed by U.S. government organizations including Department of Defense (DOD) and Department of Homeland Security (DHS) stakeholders. The DOD defines its Architecture Framework (DoDAF) as:

> "The overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate Department of Defense (DoD) managers at all levels to use architectures developed under the DoDAF in support of more effective decision-making through organized information sharing across the Department, Joint Capability Areas (JCAs), Components, and Program boundaries."[3]

The DHS Domestic Nuclear Detection Office (DNDO) describes the Global Nuclear Detection Architecture (GNDA) in this manner:

> "The GNDA is a worldwide network of sensors, telecommunications, and personnel, with the supporting information exchanges, programs, and protocols

[1] See program overview on CBD web page: https://www.dhs.gov/science-and-technology/st-cbd
[2] ISO/IEC/IEEE 42010 Systems and software engineering — Architecture description
[3] Department of Defense Architecture Framework Version 2.02. 2010. U.S. Department of Defense. https://dodcio.defense.gov/library/dod-architecture-framework/

that serve to detect, analyze, and report on nuclear and radiological materials that are out of regulatory control."[4]

While the concept of an architecture serves different purposes in DOD and DHS contexts, both definitions emphasize common themes of organization and integration, coordination, and decision support. Importantly, an architecture is not necessarily intended to override existing organizing concepts that may already be in place (e.g. existing strategy documents, or federal guidance and regulations), or displace existing capabilities. Rather, it should help users better understand how these existing elements – which constitute a baseline – fit together, and help to identify opportunities for optimization and improvement. If carried out correctly, architecture development should not be disruptive; it should ultimately enable more streamlined implementation. This report describes the process of applying architecture concepts to defense of the United States homeland against threats from chemical and biological weapons, in support of programs in the Department of Homeland Security Science & Technology Directorate (DHS S&T).

[4] Definition taken from internal conversations with DNDO.

1.2. Operational Views

There are many potential dimensions to an architecture, and these are often illustrated through graphical representations that aid communication and dialog. In DoDAF parlance, these depictions are referred to as "viewpoints" or "views." There are a multitude of viewpoint options representing different architecture perspectives including capabilities, data and information, operations, project implementation, services, standards, and the system as whole. This report – reflecting direction from DHS S&T – focuses on development of operational views, which "describe the tasks and activities, operational elements, and resource flow exchanges required to conduct operations."[5] These views include:

- **OV-1 High-Level Operational Concept**, which is a graphical/textual description of the architecture operational concept.
- **OV-2 Operational Resource Flow Description,** which describes resources flows exchanged between operational activities.
- **OV-3 Operational Flow Matrix,** which describes the specific resources exchanged and the relevant attributes of the exchanges.
- **OV-4 Organizational Relationships Chart,** which describes the organizational context, roles, or other relationships among organizations.
- **OV-5b Operational Activity Model,** which describes the context of capabilities and operational activities, and their relationships among activities, inputs, and outputs.[6]
- **OV-6c Event-trace Description,** which traces actions in a scenario or sequence of events.[7]

[5] For a complete list and description of DoDAF viewpoints, see "DoDAF Viewpoints & Models" at https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_viewpoints/

[6] The DoDAF framework includes two variations on the OV-5 viewpoint. Besides the OV-5b described in this report, there is also the OV-5a Operational Activity Decomposition Tree, which describes capabilities and operational activities organized in a hierarchal structure. Throughout the rest of this report, the term OV-5 will be used generically to describe the OV-5b.

[7] The DoDAF framework includes three variations on the OV-6 viewpoint. Besides the OV-6c described in this report, there is also the OV-6a Operational Rules Model that defines business rules constraining operations, and the OV-6b State Transition Description that describes business process responses to events. Throughout the rest of this report, the term OV-6 will be used generically to describe the OV-6c.

2. OPERATIONAL CONCEPT VIEW (OV-1)

At the highest level, an architecture helps to define a common operating picture that speaks to stakeholders in a particular mission space. The DoDAF "High Level Operational Concept" view, or OV-1, is intended to convey the mission and key components of a notional architecture; it is a communication tool intended to convey purpose and scope, without going into considerable operational detail. As a primarily visual narrative, OV-1 formatting varies considerably according to the mission area and stakeholder requirements.[8] In general, most include the following elements:

- A statement of purpose or mission, often derived from policy/strategy documents.
- A definition of the threat or hazard being managed or mitigated by the architecture.
- Identification of key defensive or operational priorities.
- The operational interaction between various architecture elements or components.

This view is useful for a wide range of potential audiences, including decision makers and external stakeholders (e.g. the public and media) that only have time or expertise for the highest-level details. Visual impact is critical for an OV-1; graphic designers should be included from the beginning of development.

An example of an OV-1 depicting a notional biological defense architecture is shown below (Figure 1). At the top of the graphic, the fundamental goal of the architecture is highlighted (public health and safety). Below that, the general nature of the biological threat (malicious, accidentally, and naturally occurring) and specific infection pathways (human, animal, insect, etc.) are both highlighted. Specific geographic defensive priorities are further highlighted, including transit pathways (roads, aviation, seaports, etc.) and potential targets (critical infrastructure, special events, government, etc.). The second OV-1 illustrated below (Figure 2) depicts a chemical defense architecture. While basic elements of the graphic are similar, the threat is defined slightly differently (namely, there are no naturally occurring chemical threats), and rather than infection pathways, the graphic highlights how chemicals may be employed in scenarios exploiting their toxicity, explosivity, or flammability. Finally, both OV-1s emphasize collection, communication, synthesis, and analysis of information streams supporting various stakeholders (federal, state, local, and tribal) as a key operational interaction in the architecture.

[8] See DoDAF OV-1 guidance: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/DoDAF20_ov1/

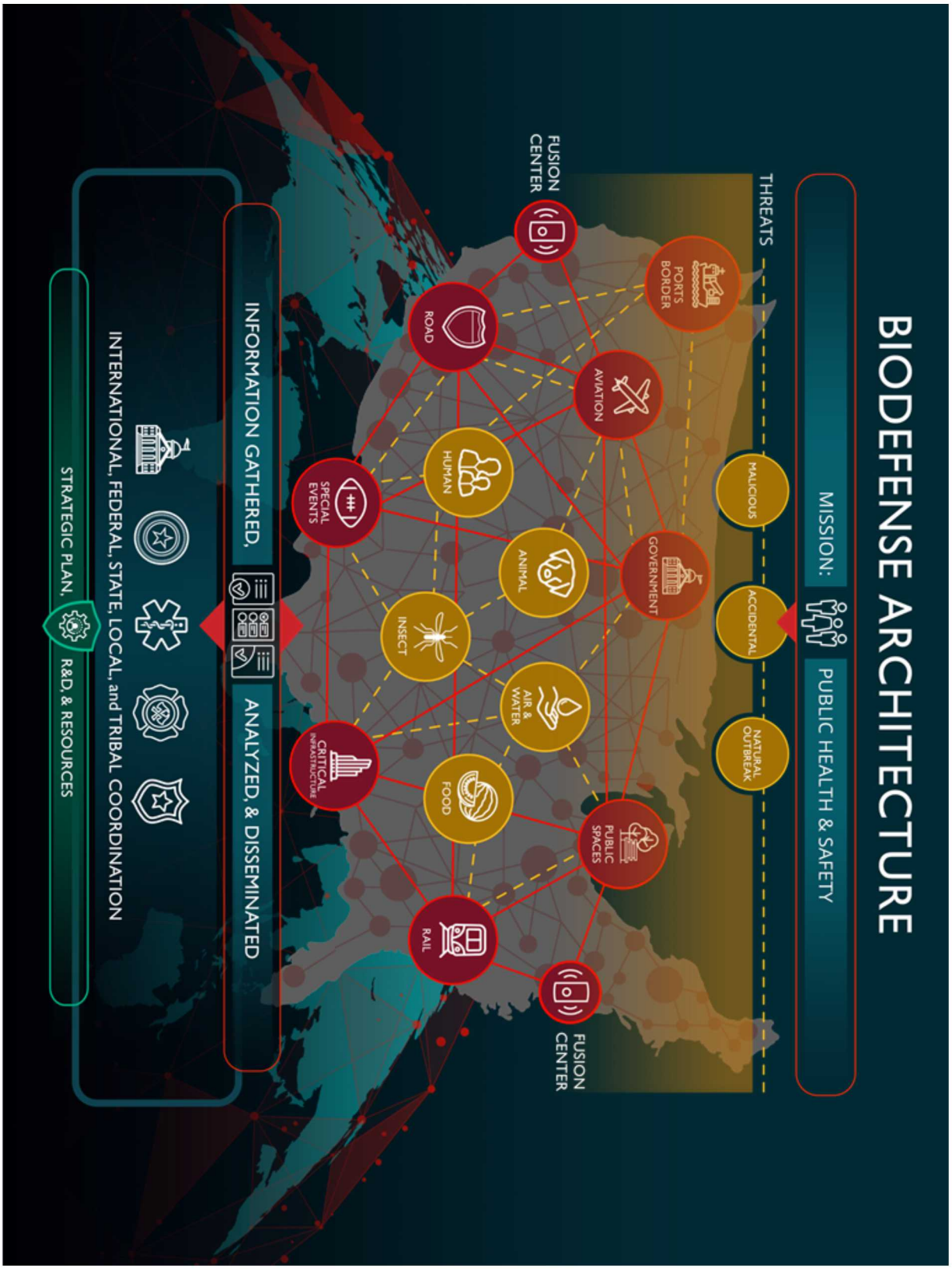

Figure 1: Biodefense Architecture OV-1

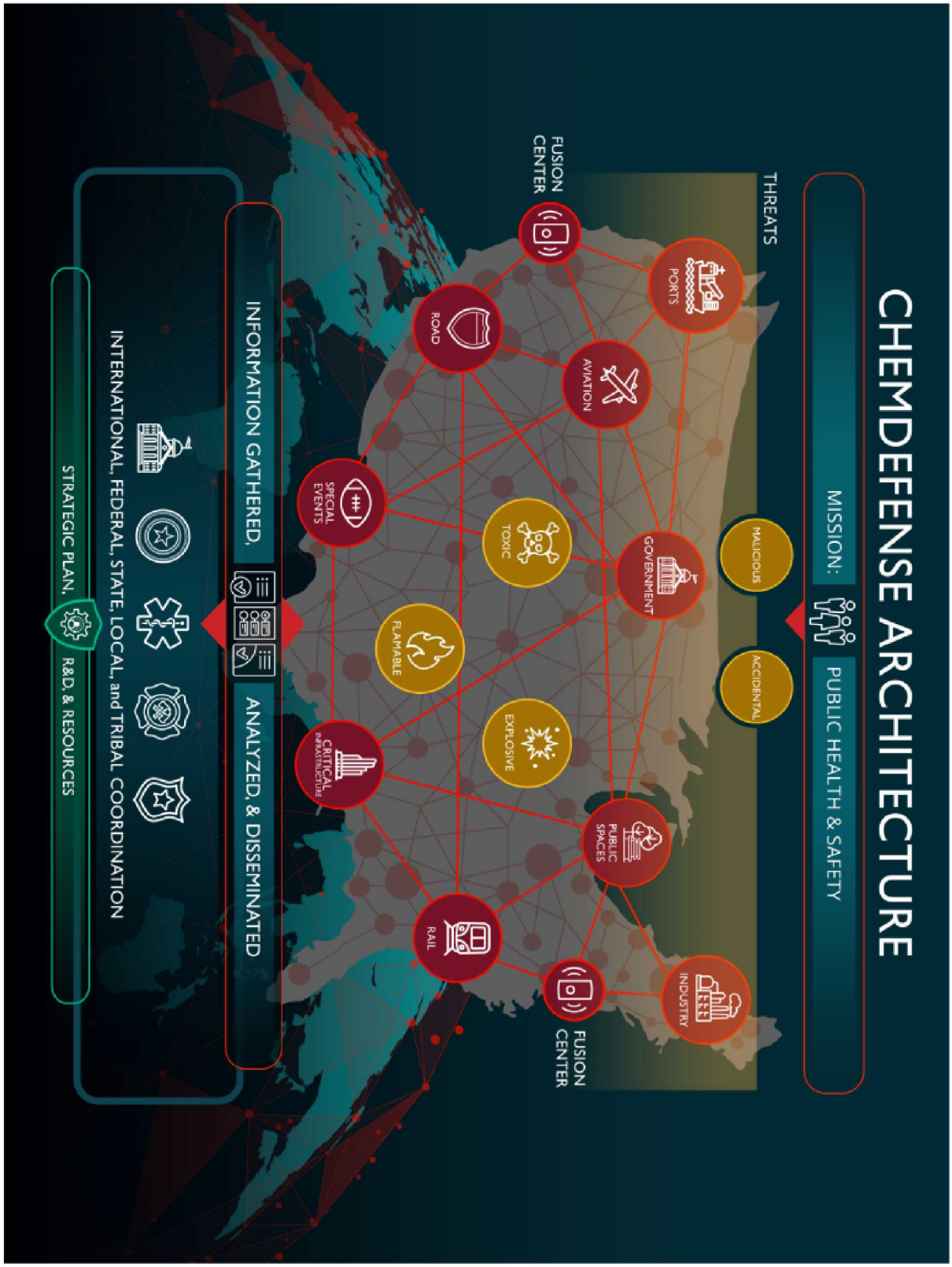

Figure 2: Chemdefense Architecture OV-1

3. OPERATIONAL RESOURCE FLOW (OV-2) & FLOW MATRIX (OV-3)

The Operational Resource Flow view (OV-2) illustrates the movement of resources among broadly defined functional groupings of organizations in the architecture, as defined by strategy documents or consensus among stakeholders.[9] Depending on the scope of the architecture, or specific questions that need to be addressed, there may be value in separating organizations at different levels, include federal, state, local, tribal, and even international functional roles. The example below (Figure 3), addressing detection of biological security events, includes grouping for both federal and state/local entities. For example, at the national level, the "National Security" grouping might include entities like DHS, the Department of Defense (DOD), and the National Security Council (NSC). Local Response entities at the state/local level might include entities like Police, Fire, and Emergency Medical Services.

Figure 3: Assignment of Functional Roles

The OV-2 further maps the expected or known flow of resources between these functional groupings in relation to prevention, detection, and response activities, as indicated by directional "needlines". The figures below are examples of completed OV-2s representing detection of an anthrax release in an urban subway environment (Figure 4) and chemical prevention/protection in an urban area (Figure 5). Each needline represents a resource that should pass from one functional group to another in support of bio detection. For example, to support detection of biological outbreaks

[9] See DoDAF OV-2 guidance: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_ov2/

(Figure 3), local public health offices may be expected to provide notification of anomalies (e.g. patients with suspicious symptoms) to national public health authorities, along with situation updates as events progress. National authorities are then expected to provide response guidance as needed. The resources associated with each needline can include data/information, guidance, and even physical assets.

It is useful to contrast the biological threat-oriented OV-2 with its chemical threat-oriented counterpart (Figure 4). The concept of detection is less salient in chemical security, where the release of a chemical agent will likely lead to immediate casualties and trigger response efforts; it is less likely there will be lead time for a distinct "detection phase" (by contrast to a biological release, which might take days or weeks to manifest in terms of attributable patient symptoms or casualties). Rather, chemical security stakeholders focus on prevention and protection measures that will either prevent a chemical release from happening in the first place (e.g. intelligence sharing and private industry inventory control), or facilitate a rapid response in the event of a release (e.g. Concept of Operations development and exercises).

The OV-2 is augmented by an Operational Resource Flow Matrix (OV-3), which provides additional descriptive detail for each needline, taken from planning documents and/or dialog with stakeholders. At a minimum, the OV-3 contains a description of the resource being passed from sender to receiver, and the operational activity associated with use of that information. For example, in the first line of the OV-3 shown below (Table 1), the SD1 needline is associated with requirements for monitoring and reporting that are passed from the National Public Health authorities to National Regulatory and Inspection authorities. The National Public Health authorities set and communicate these requirements, while the Regulatory and Inspection authorities incorporate those requirements into their regulatory inspection process.

In addition to this basic information, users may add additional detail to support more fine-grained analysis of resource flows. This could include requirements related to the quality of the information/resource being shared, the timeliness of movement, any interoperability considerations (e.g. data formatting standards), and classification/sensitivity associated with the resource. This information can inform subsequent analysis activities, including gap analysis and optimization.

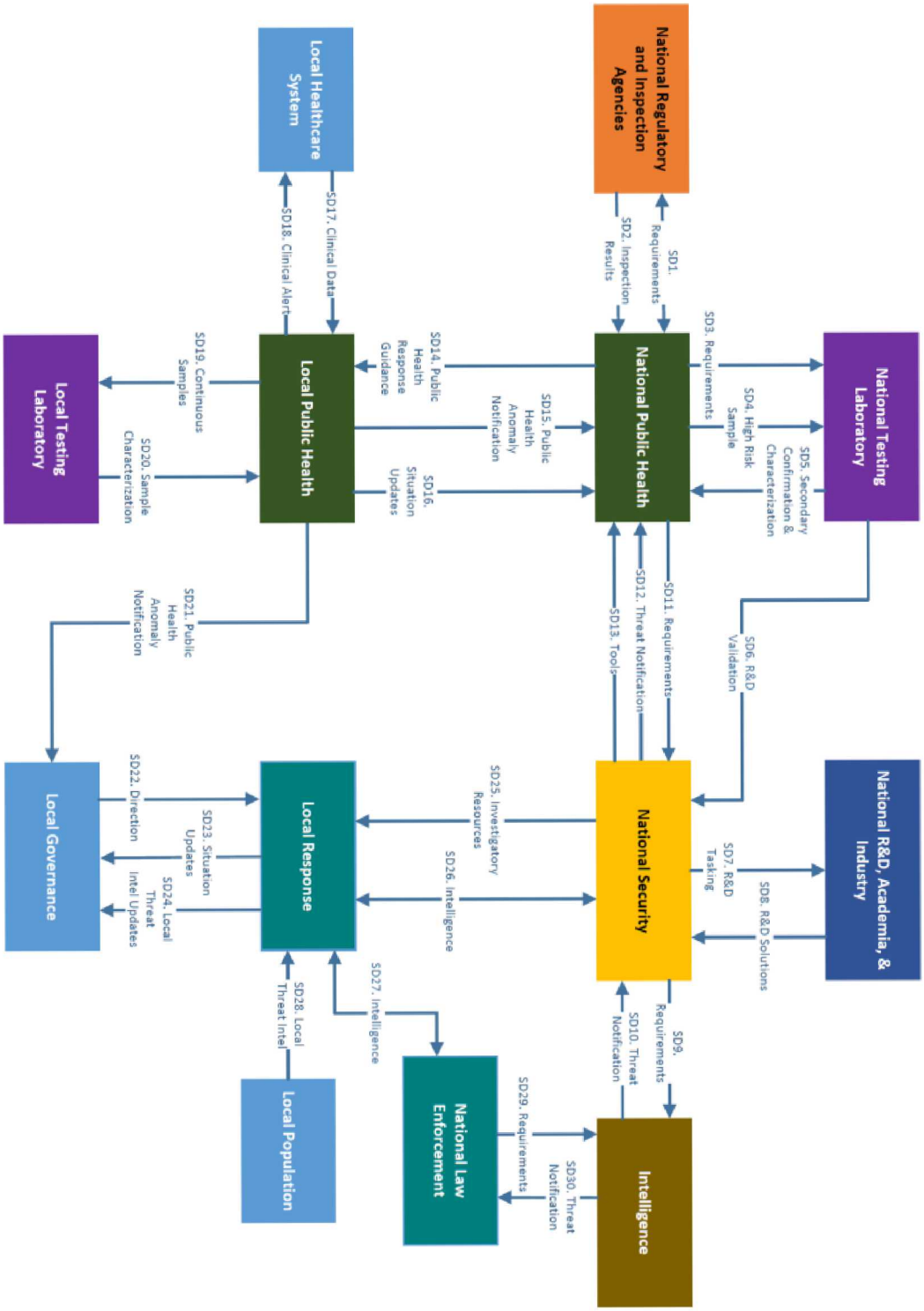

Figure 4: Urban Underground Transportation System Biological Agent Detection OV-2

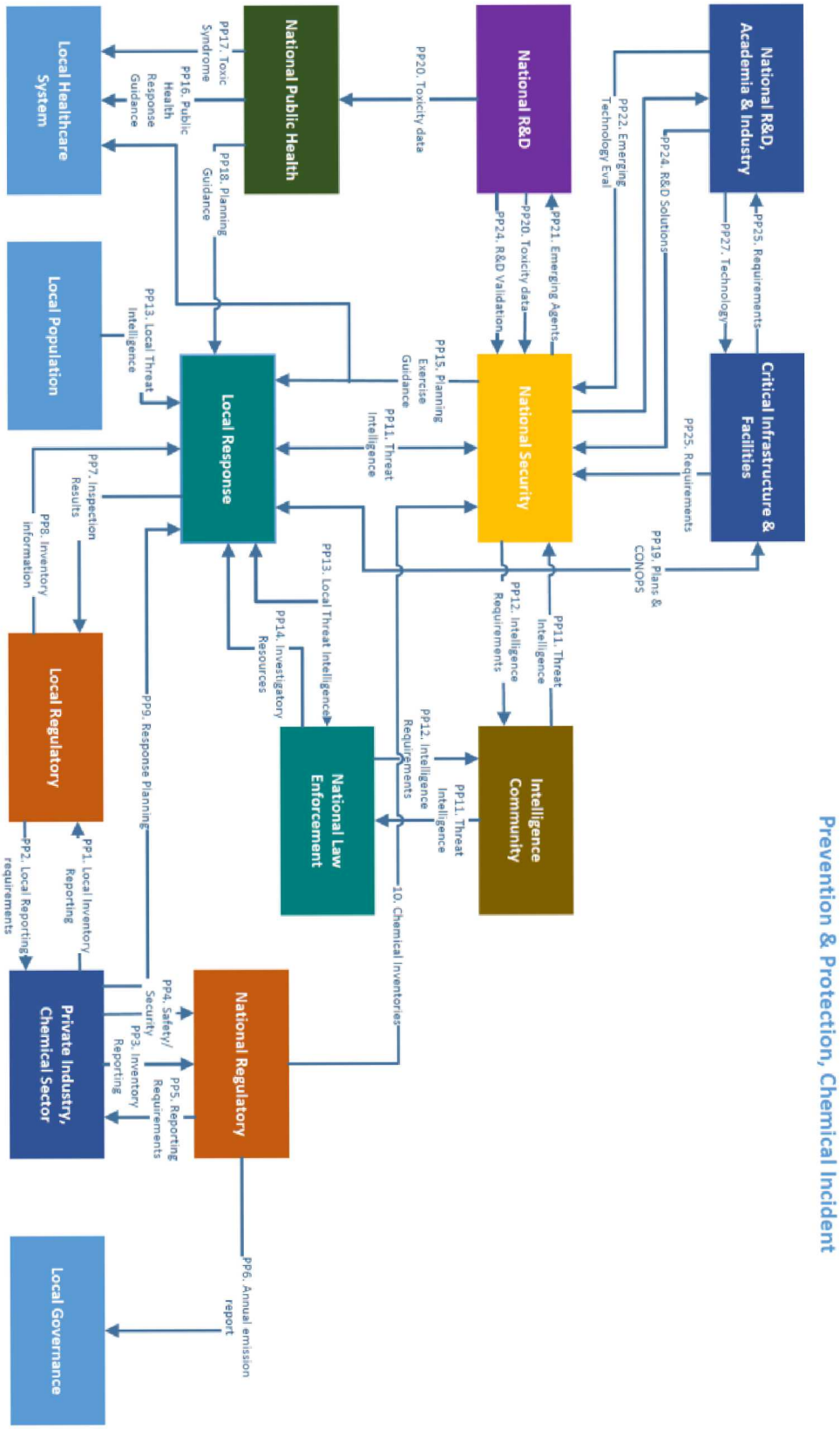

Figure 5:Chemical Prevention & Protection OV-2

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

Table 1: Biological Detection & Surveillance OV3

4. OPERATIONAL RELATIONSHIP VIEW (OV-4)

While the OV-2 and OV-3 illustrate relationships between broad functional groupings or categories of architectures stakeholders, the Organizational Relationship View (OV-4) is intended to highlight individual architecture stakeholders and their more specific relationships relative to one another. There are many different options for illustrating such relationships; the most basic is an organizational hierarchy. However, not every architecture can be adequately described in terms of hierarchical organizing concepts.

In the example illustrated in Figure 6 below, stakeholders are associated with a strategy pillar or goal of "threat awareness" (center circle), as defined in a strategy document. They are further categorized by function (first ring of colored circles – national security, intelligence, academia, regulatory, etc). The actual stakeholders (second ring of colored circles) are decomposed from the highest-level authorities (e.g. cabinet-level agencies) down to subordinate offices, and potentially even to individual programs and implementers. Auxiliary functional relationships that exist outside formally define hierarchies can also be highlighted. For example, in this OV-4 the Federal Bureau of Investigation is illustrated in two places; the first as a subordinate of the Department of Justice (its primary relationship), and the second as a participant in intelligence activities (where the lighter coloration indicates a secondary relationship).

The ultimate purpose of this mapping is to more clearly define the functional lanes in which stakeholders ostensibly operate; this information can be used to identify (and ultimately deconflict) overlaps, as well as identify opportunities for collaborative partnerships that may not have been immediately evident.

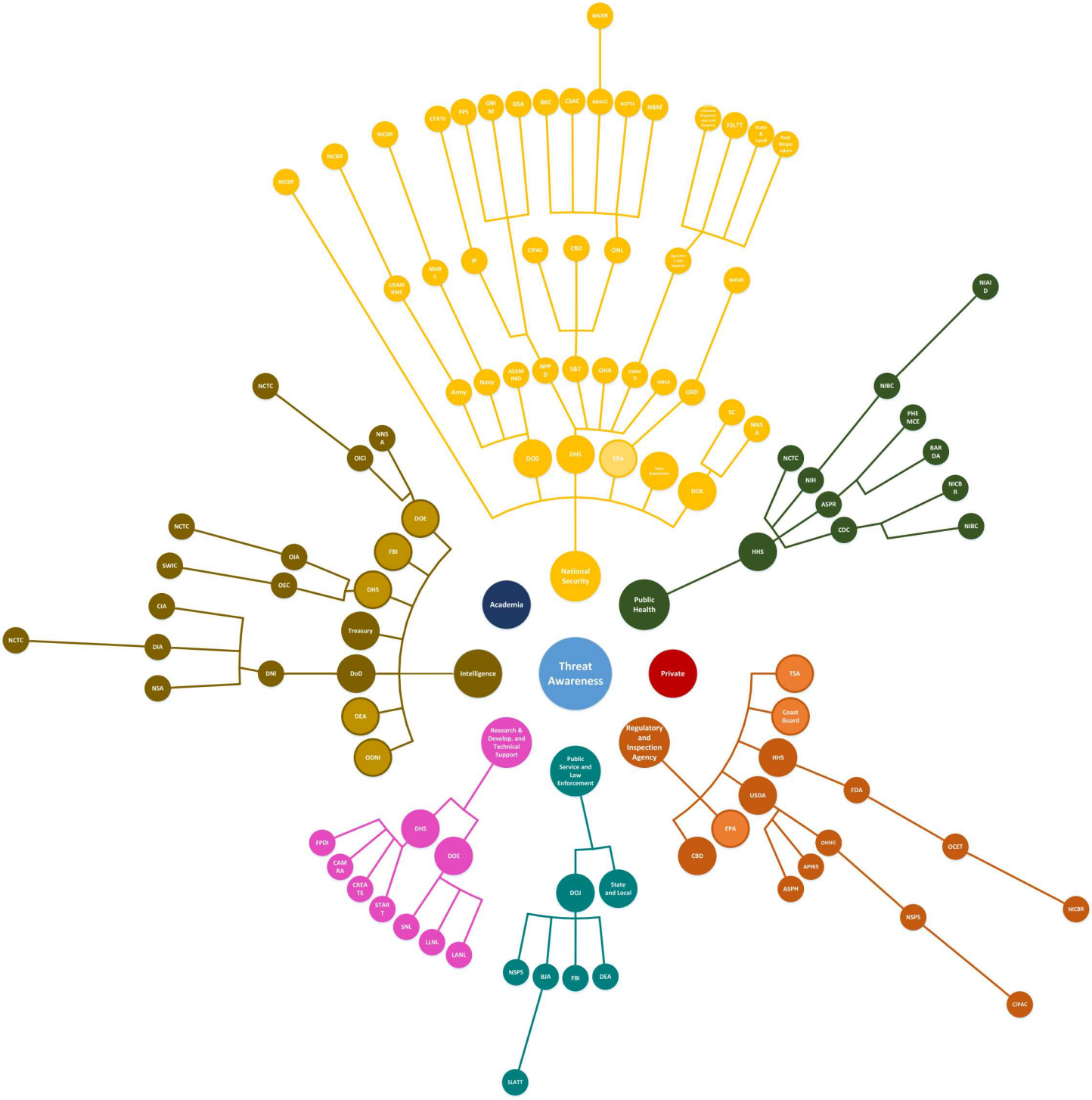

Figure 6: Biological Threat Awareness OV-4

5. OPERATIONAL ACTIVITY DECOMPOSITION (OV-5)

In some cases, it may be desirable to illustrate stakeholder roles and responsibilities in the event of a specific scenario; this is the purpose of an Operational Activity Decomposition, or OV-5.[10] The OV-5 details the sequence of activities undertaken by architecture stakeholders in a given operational context; this context is usually broadly defined, without reference to a specific geographic location or locality. OV-5 development begins with selection of an operational scenario. In the case of chem-bio defense, this will likely include an assumed combination of a threat and target, along with the operational phase under consideration (e.g. prevention, detection, or response). The first example below (Figure 7) illustrates the detection phase of a subway anthrax release in an urban area. The three red boxes indicate different detectable indicators that an attack has taken place; each is associated with different follow-on actions (though in this case, all eventually lead to a confirmation or non-confirmation of the event). This information is usually drawn from documented Concepts of Operation (CONOPs) and/or stakeholder consultation (in this case the information was drawn and genericized from documents drafted by state and local authorities in a major U.S. metropolitan area).

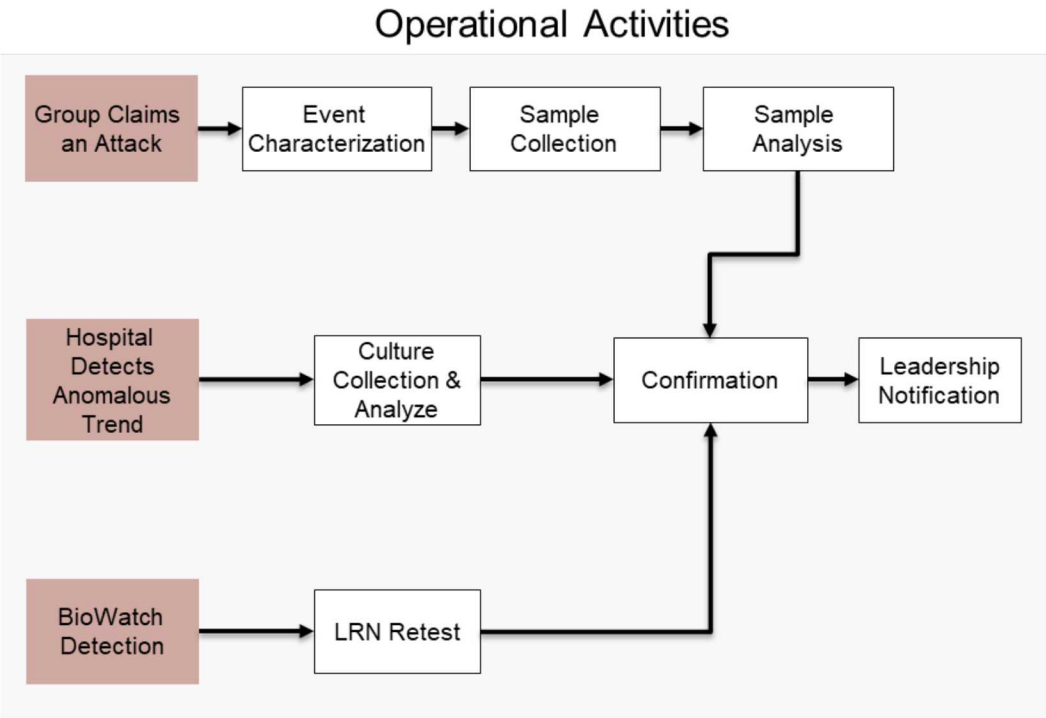

Figure 7: Operational Activities as Defined for Urban Underground Transportation System Biological Agent Release OV-5

The OV-5 further situates each activity within a functional-organizational lane (national security, public health, etc.), indicating which stakeholder set is ostensibly responsible for that activity; this is illustrated in Figure 8, below. It is not uncommon for implementers to have conflicting, mistaken, or misinformed impressions of their

[10] See DoDAF OV-3 guidance: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_ov3/

roles and responsibilities in a given incident scenario, and this view helps facilitate a conversation to clarify – and potentially even realign – those roles. It is better to work out such differences in a structured way under normal conditions, rather than ad hoc at the time an incident takes place.

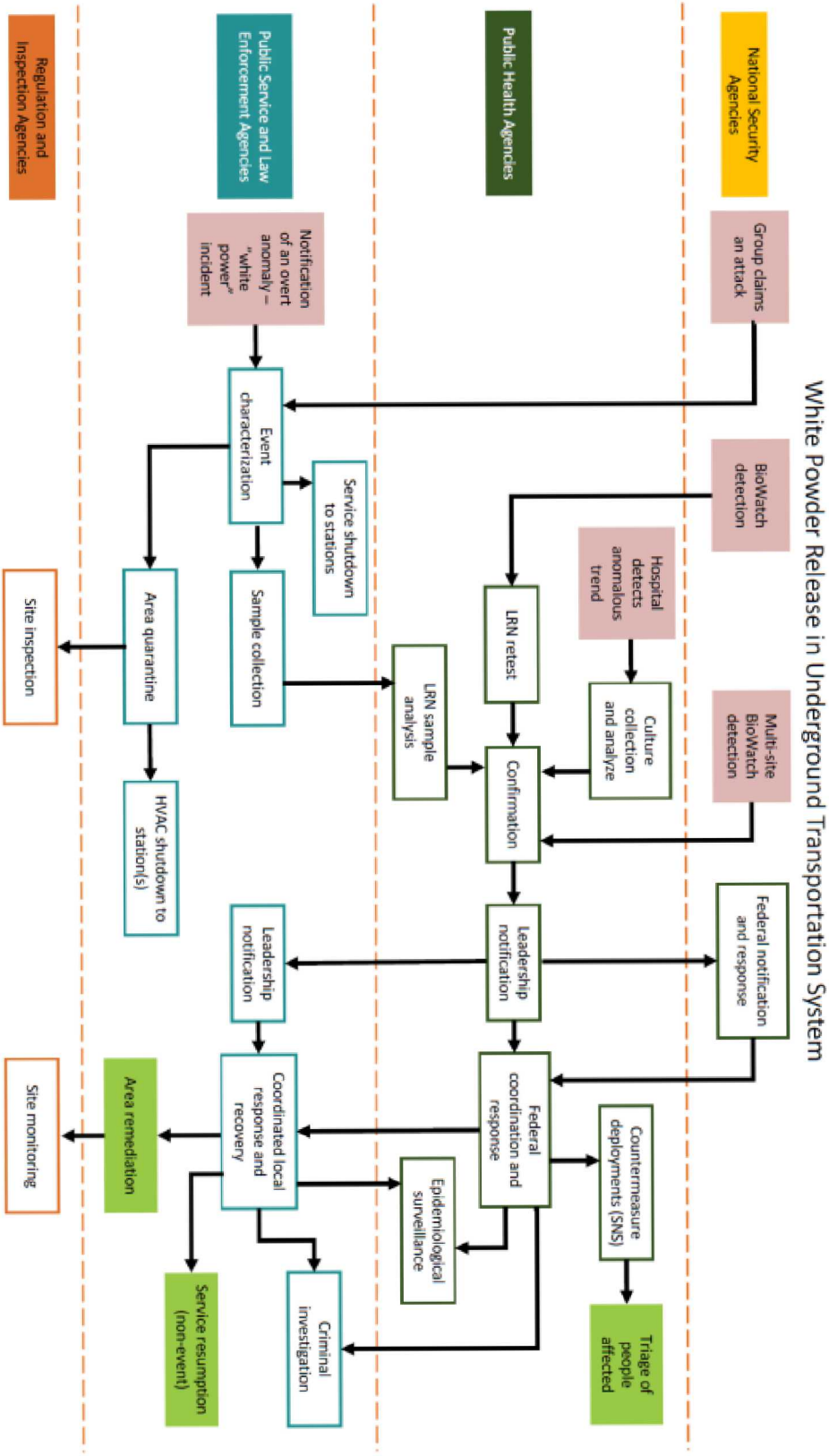

Figure 8: Urban Underground Transportation Bioagent Release OV-5

6. OPERATIONAL EVENT-TRACE (OV-6)

In some cases, more detail may be required for understanding and analyzing decision processes in even more specific operational circumstances; this is the role of an Operational Event-trace, or OV-6. Like an OV-5, the OV-6 begins with an operation scenario.[11] However, the scenario is more specifically situated within a real-world locality, referencing individual stakeholders (rather than broad functional groupings, as in the OV-5). The OV-6 also includes more detail regarding time and sequence. The examples below (Figure 9) situate the urban anthrax release within a subway, in which detection take place via a BioWatch detection system. The horizontal axis of the OV-6 lists the different stakeholder organizations for the locality. The vertical axis is a timeline; this can be defined in terms of discrete units (e.g. hours, minutes, days), or (as in this case) more broadly defined operational phases, depending on preference and available guidance.

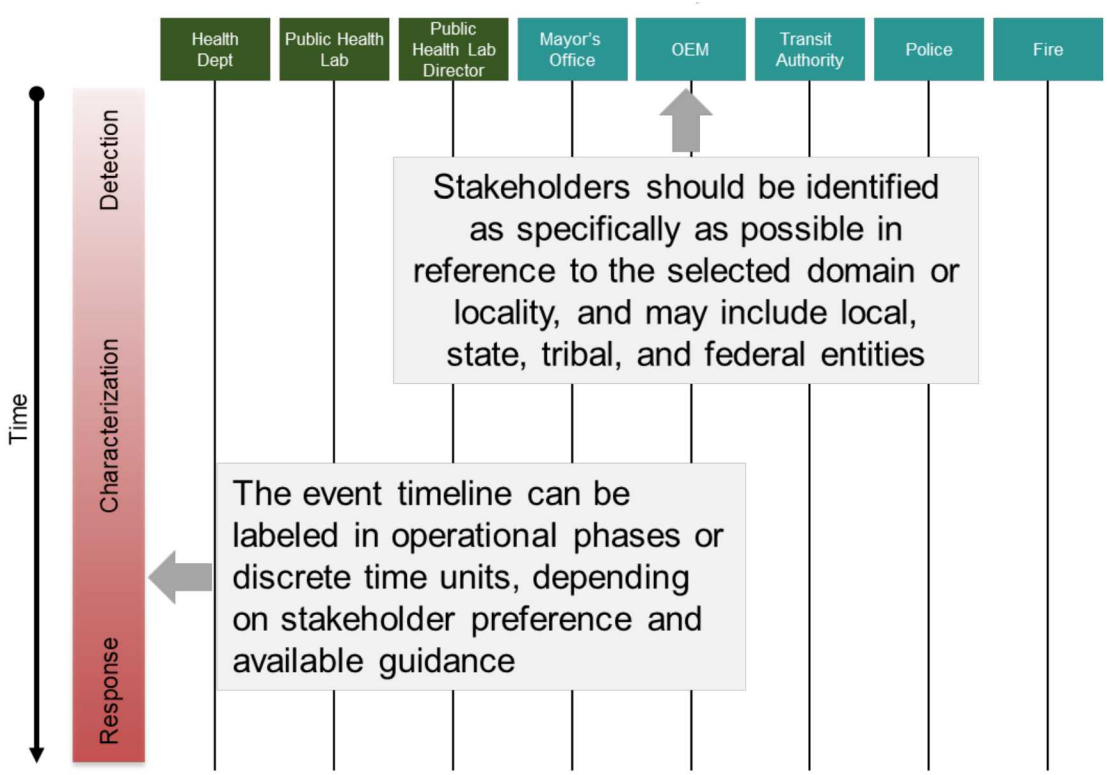

Figure 9: OV-6 Axes, Detection of Urban Bioagent Release by BioWatch Detection System

Drawing from operational guidance, the OV-6 then lays out the sequence of actions taken over time in the operational scenario. Each labeled horizontal line represents an operational action. Relevant stakeholders are indicated with a dot on the line. An open

[11] See DoDAF OV-6 guidance: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_ov6introduction/

dot indicates an organization has primary responsibility or authority for the action; a closed dot indicates that an organization is party to the action (note that if there is no dot, then an organization is not party to the action – even if that action line passes by the organization). Actions are punctuated by key decision points in the event timeline, indicated by a diamond. Figure 10 below shows a partial event trace representing the detection phase of the anthrax event.

Figure 11 below shows the full event-trace, from initial detection through executive branch declaration of an emergency (which would then transition to the response phase and a different OV-6). Depending on the scenario and the locality, an event-trace can be very detailed; the example illustrated here is probably somewhere in the middle-range of detail and complexity. OV-6 construction requires access to current planning documents, and ideally close consultation with stakeholders. The development of an OV-6 itself provides an opportunity for interagency engagement and development of shared understandings regarding operational details and responsibilities. Like many architecture products, the value is not necessarily in the final product, but in the process for getting to that product. A completed OV-6 also has analytical utility; it can support identification of procedural inconsistencies, bottlenecks, gaps, and overlaps. This information can then be used to support optimization of prevention, detection, and response processes.

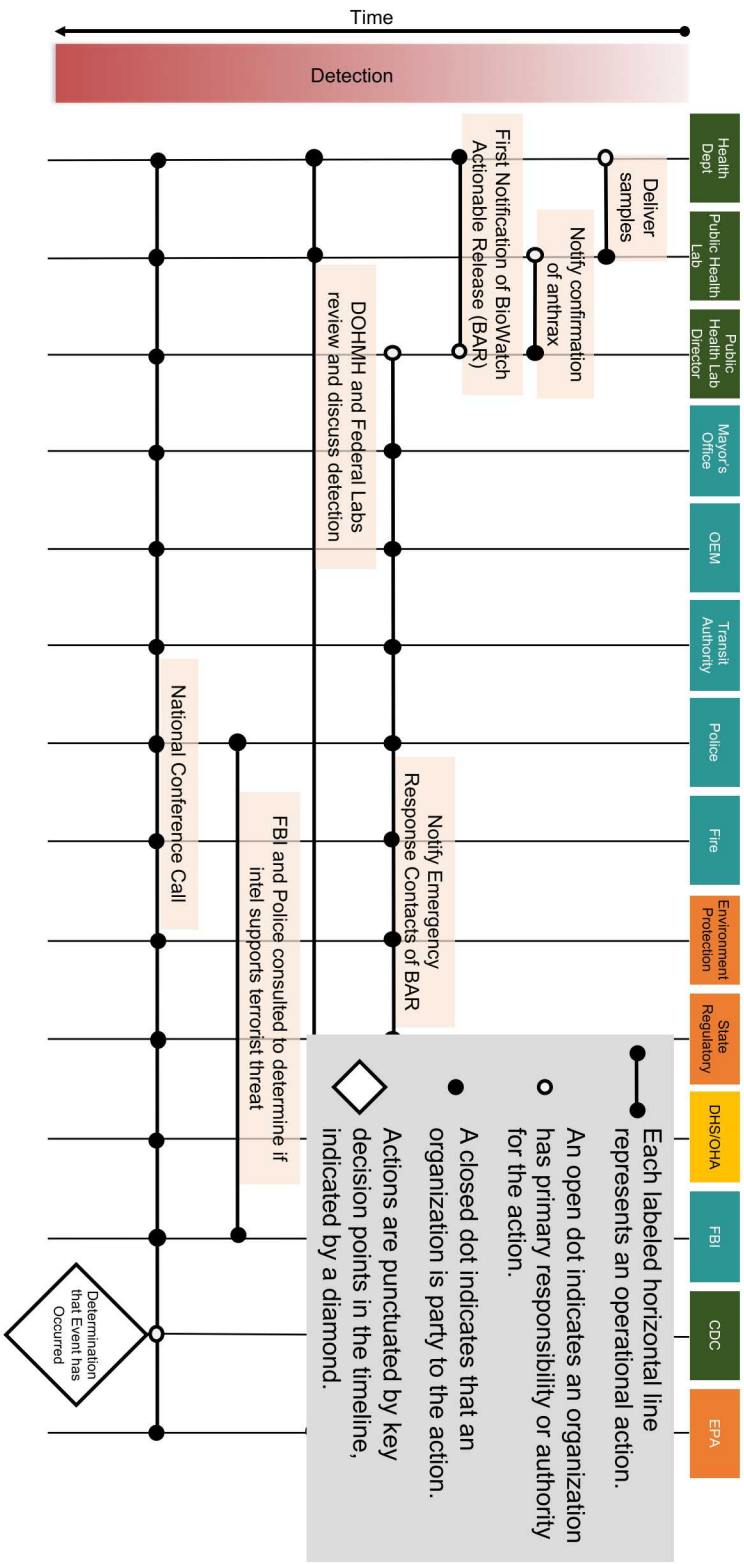

Figure 10: Partial OV-6 Operational Event-trace, Urban Underground Transportation System Biological Agent Event

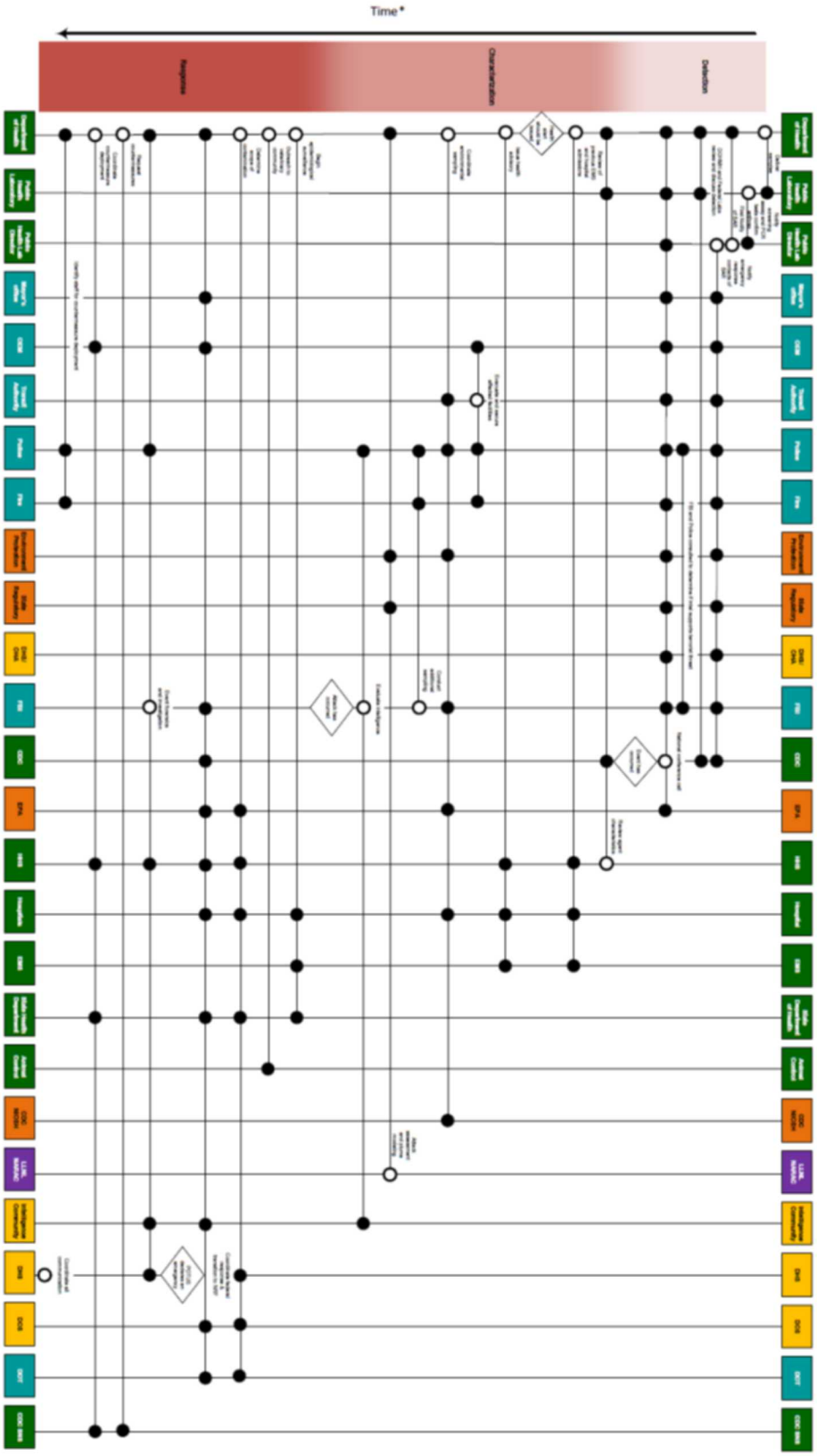

Figure 11: OV-6 Operational Event-trace, Urban Underground Transportation System Biological Agent Detection Event

7. ARCHITECTURE APPLICATION

An architecture provides more than just organizational guidance; it also has analytical utility in supporting identification of capability requirements and priorities. This can be a challenging task in the chem-bio defense field; implementers are often presented with a range of options for filling capability needs, often by a mix of public sector assistance providers and private vendors. In addition to meeting their own operational needs, implementers need to further select capabilities that complement, and/or are compatible with, those of other organizations operating in the same operational or jurisdictional domain.

The OV-3 Operational Resource Flow Matrix is particularly useful as a starting point for evaluation of existing capabilities. Table 2 below shows selected rows from a notional OV-3. Three additional columns have been added. The "Capability Requirement" and "Capability Inventory" columns support qualitative gap analysis. The former column specific requirements for resource and information sharing for a given needline, which might be derived from planning documents, concepts of operation, or even legislation. The latter column is populated with an inventory of deployed capabilities, which can then be evaluated against the requirements. Gaps are highlighted in red. The final column, S&T Program Support, lists notional programs in the S&T portfolio. Populating the OV-3 with this information allows architecture planners to analyze the degree to which a given program portfolio is targeting identified gaps, and where addition investments may be needed.

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	• 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	Ongoing BioWatch 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

Table 2: Notional Program Portfolio Analysis

More advanced analysis options are also available. To prioritize investments and identify gaps, the effectiveness of the defense architecture can be evaluated in the context of its impact on risk. An influence matrix analysis (shown in Figure 12) is one approach for evaluating a defense architecture against a threat scenario at a high level. Along the diagonal of the matrix is a series of scenario elements corresponding with

an attack timeline, starting with elements of the threat on the top left quadrant, followed by elements of the defense architecture in the bottom right quadrant.

The OV process provides a high-resolution characterization of the defense architecture quadrant. A parallel framework can be created for the threat quadrant, describing an attack scenario comprising agent, target, and dissemination method. The threat framework may be derived from formal terrorism risk assessments, or other threat and risk analyses. Various analytical techniques can be applied – e.g. subject matter expert elicitation, formal modelling and simulation, or tabletop exercises – to evaluate the degree of threat mitigation afforded by the defensive architecture, and also the recursive influence that defensive actions might have on adversary behavior (and vice versa).

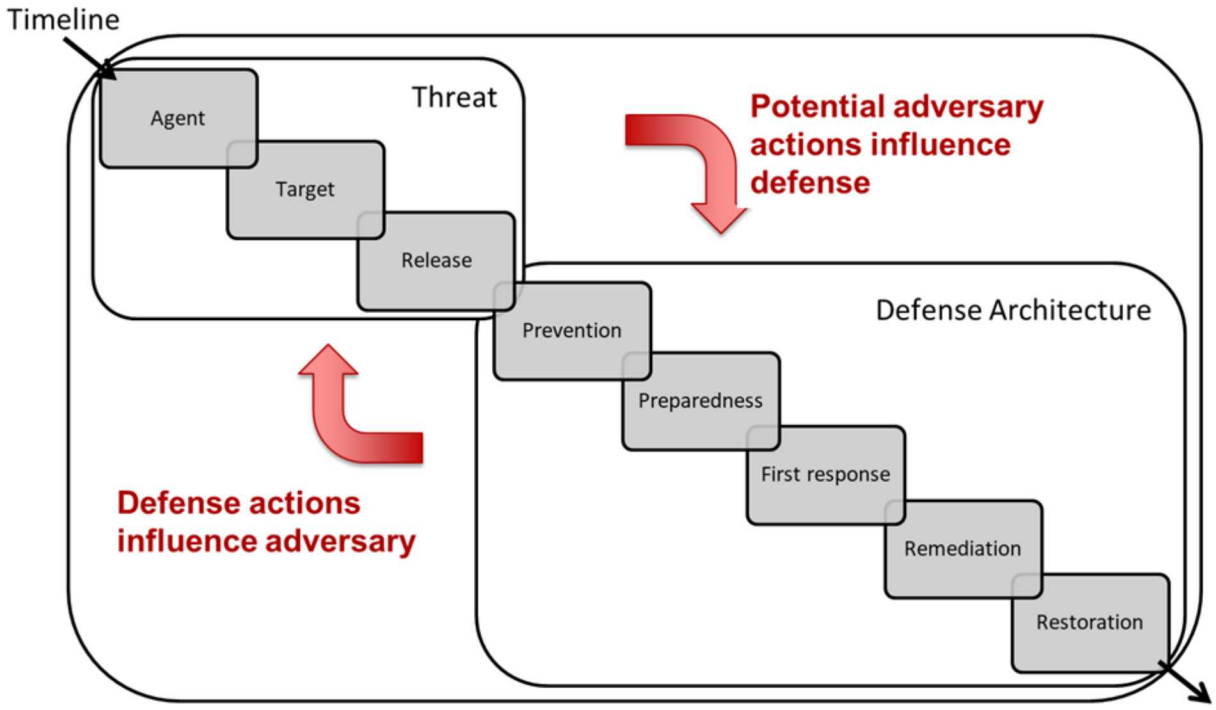

Figure 12: Influence Matrix-based Risk Mitigation

These are just two examples of the analytical utility potentially afforded by application of architecture concepts. Such analysis was outside the scope of funded work, but is a logical extension that might be considered for future architecture development at DHS.

In closing, it should be emphasized that there is no "one size fits all" template for an architecture, or related analysis. Every organization enters into the development process with unique capabilities, challenges, and implementing contexts; these details often translate into products that look very different from organization to organization. Moreover, much of the value-added from the development process comes not from the graphics or final analysis products (though these are important), but from the

conversation and iteration that takes place between stakeholders. These conversations ensure that all perspectives and interests are accurately represented, and also help to promote broader awareness and relationship development that can be valuable in the field when an actual chem-bio event takes place.

Finally, architecture development is not a “one and done” process. Threats evolve; so do the organizations, technologies, policies, and other features of the implementing environment. Just like strategy, the assumptions and organizing principles underlying an architecture should be periodically revisited and revised to reflect these changes.

DISTRIBUTION

Email—External (encrypt for OUO)

Name	Company Email Address	Company Name
John Fischer	John.fischer@hq.dhs.gov	DHS S&T
Dave Shepherd	Dave.shepherd@hq.dhs.gov	DHS S&T

Email—Internal

Name	Org.	Sandia Email Address
Nataly Beck	8621	nlbeck@sandia.gov
Victoria VanderNoot	8621	vavander@sandia.gov
Sheryl Hingorani	8710	slhingo@sandia.gov
Benjamin Bonin	8712	bjbonin@sanida.gov
Trisha Miller	8712	millert@sandia.gov
Nerayo Teclemariam	8712	nptecle@sandia.gov
Julie Fruetel	8714	jfruet@sandia.gov
Patricia Hernandez	8714	pmphern@sandia.gov
Janson Wu	8718	jwu@sandia.gov
Technical Library	01177	libref@sandia.gov

This page left blank

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.