

Statement of
Steven I. Cooper
Chief Information Officer
Department of Homeland Security

before the

Committee on Government Reform
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

October 8, 2003

Mr. Chairman and Members of the Subcommittee:

I am pleased to appear before the Subcommittee today, and want to thank the Chairman and members of the Subcommittee for giving me the opportunity to talk about the Department of Homeland Security (DHS) Enterprise Architecture (EA) planning project. I am very pleased to announce to you that in September of this year, we completed the first version of our target EA and are already beginning to implement the objectives of our EA Transition Strategy. The EA will help DHS align Information Technology (IT) investments with its mission and business needs, and improve data sharing and interoperability with its many information sharing partners, such as other Federal agencies and State, Local, and Tribal governments.

In my previous testimony I discussed the vision and strategy of DHS and how that strategy must be supported by a disciplined capital planning and investment control process that is guided by a business-driven EA. DHS' strategy identified major initiatives such as information integration across the federal, state, and local governments, private industries, and citizens; common standards for electronic information; improved communications; and reliable public health information. The EA captures this strategy and describes a target information management infrastructure that will be dramatically different from the one we have today—one that will provide timely, accurate, useful, and actionable information to all individuals who require it.

We have accomplished something unique in Federal government: We designed and delivered a comprehensive—and immediately useful—target EA in under four months. Our EA is enabling us to make decisions about our IT investments now, even as we continue the hard work of developing greater detail, reaching deeper to find more opportunities for consolidation, and beginning to develop new and improved mission support capabilities. I would like to now provide an overview of the DHS EA and discuss how we are using our EA today, as well as how it is aligned to the Federal EA reference models and E-government initiatives.

Introduction to EA

Mission performance depends on providing operational decision makers with appropriate, accurate, and timely information upon which to base their decisions. IT is a significant contributor to providing such information. The challenge is putting in place a modern, adaptable, and interoperable set of applications to aid in improving mission performance.

Although IT cannot address all the challenges faced by DHS and its homeland security partners, alignment to business activities will improve the Department's overall ability to execute its mission.

DHS embarked on its EA planning project as a beginning point for integrating its business processes, data, application systems, and IT—to transform from an organization composed of 22 formerly separate agencies and their various assets, to an organization with a unified, interoperable infrastructure and a modern, adaptable, and interoperable set of IT applications based on the business needs of DHS.

Documenting our business and information needs through EA planning enabled us to highlight overlapping and duplicative initiatives. For example, we have identified at least eight existing initiatives supporting Port of Entry management that can be unified, leading to cost savings. We have begun identifying areas where we can leverage and reuse legacy systems. In the same Port of Entry management example, we have identified at least three existing systems that have capabilities that can be reused to meet that business need. And we have begun identifying mechanisms for sharing information not only within DHS, or even within the federal government, but also with the first responder community, and state, local, and tribal governments to support the broader homeland security enterprise.

Our EA provides the vision, concepts, and structure to enable, enhance, and increase the efficiency of DHS. I believe that it is unique in many respects. First and foremost, it is business driven; that is, it is based on the mission needs of DHS that, in turn, drive the target IT architecture. Also, the Target EA has been constructed to provide the necessary agility to enable rapid changes in response to new threats through flexible component- and service-based applications. It is based on the reuse of components to reduce the costs of IT development, and business and technology patterns to ensure repeatability of common processes.

Our DHS EA Team has produced a conceptual-level EA. It provides a high-level view—a critical beginning as our initial EA requirement was to identify and drive opportunities for consolidation and interoperability. I want to point out that even though it is conceptual, it is actionable. In fact, we are using our EA transition strategy to focus on early quick hits and development of initial component capability in FY04. The first components that we will create (whether we build new or modify existing investments) are those which are reused most frequently, and serve as foundational capabilities. We are also using our EA plan to inform our FY05 budget process and it will be even more instrumental in making IT investment decisions in the FY06 budget process.

Support for Federal Initiatives

EA is one of the means by which visibility into IT assets can enable the federal government to find business and financial efficiencies. Our alignment to the Office of Management and Budget's Federal Enterprise Architecture and our transition to e-government initiatives are discussed below.

Support for the Federal Enterprise Architecture

The Office of Management and Budget (OMB) Federal Enterprise Architecture (FEA) is an approach and framework that provides guidance to federal agencies in developing their EAs. It provides a common structure and vocabulary for federal EAs, so that they may be analyzed and compared to identify commonality and duplication across agencies. Our EA planning project was driven by the concepts and products of the OMB FEA Reference Models. We have aligned the various EA artifacts with the five FEA Reference Models: the Business Reference Model, the Data and Information Reference Model, the Service/Component Reference Model, the Technical Reference Model, and the Performance Reference Model. And, more importantly, we have embraced the two FEA foundation concepts: Line of Sight for program effectiveness and Component and Service Based Architectures for effective reuse and repeatability.

Business Reference Model. The FEA Business Reference Model drove the development of our business model. Several of the Business Reference Model Lines of Business are directly applicable to DHS (in particular, Homeland Security and Disaster Management). For all other business activities within the DHS business value chain level, there is a one-to-one link to the Business Reference Model Lines of Business. The EA Business Model includes a matrix that shows the relationship between our business activities and the Business Reference Model Sub-functions. It is important to note that every business activity in the EA Business Model is mapped to a Business Reference Model Sub-function. As a result of this alignment, OMB should be able to readily identify functional commonality of DHS with other federal agencies.

Data and Information Reference Model. The Data Reference Model consists of a layered model for decomposing collections of information, from Subject Areas down to Data Objects and their properties. We adopted this approach and classified the information required to support the homeland security business activities at the Subject Area and Data Object levels. Further decomposition and description of the data objects will be performed in the next phase of the EA process. Our Data Architecture aligns with the Data Reference Model concepts by providing a common, consistent way of categorizing and describing data to facilitate data sharing and integration.

Service Component Reference Model. The DHS EA project has fully embraced the FEA Service/Component Reference Model's component-based approach to the reuse of applications, application capabilities, components, and business services across the federal government. OMB created the Service/Component Reference Model specifically to identify service components and their relationship to the technology architectures of federal agencies. We leveraged the Service/Component Reference Model in two important manners: (1) the structure of our Application Architecture is a set of interworking components that has direct ties to the Service/Component Reference Model, and (2) our Technology Architecture applies a set of technology patterns that is derived directly from the technology aspects of the reference model.

The Application Architecture has been constructed to leverage reusable components that can be acquired once and used to provide services to many applications. It shows the structure of this component reuse. From the set of component architecture diagrams, it can be seen that there is a significant opportunity to apply this reuse concept throughout DHS (and across other

government agencies). The result should be considerable cost savings, as well as greatly improved interoperability and flexibility of applications.

The Technology Patterns of our EA are repeatable solutions to recurring technical challenges. These patterns employ technologies described in the DHS Technical Reference Model (discussed below) and provide capabilities as described in the FEA Service/Component Reference Model. For example, the Business Intelligence/Data Warehouse technology pattern of our EA aligns with the Business Intelligence Service Type of the FEA reference model.

Technical Reference Model. The initial formulation of the DHS Technical Reference Model began with the taxonomy as well as the technical services, protocols, and interfaces specified in the FEA Technical Reference Model. The DHS model extends and refines the FEA model where necessary to reflect the additional functional and technology requirements of DHS. In deriving the DHS model from the FEA model, we have also made adjustments to better align the technology categories with the physical layering of services that exist in vendor and open source products. The Domain level (Tier 3) categories of the DHS model have all been mapped to the FEA model, so that comparisons can be directly made with the technical reference models from other agencies.

Performance Reference Model. Although this FEA reference model was still under development during our EA planning project, an initial attempt was made to align our Business Model with the intent of the Performance Reference Model, based on draft materials provided by OMB. Specifically, the Business Model includes a table that defines the outcomes or measurement categories and corresponding indicators (metrics) for each cross-cutting, corporate activity defined in the Homeland Security Value Chain. Measurement categories are defined for each activity in six areas: Mission and Business Results, Customer Results, and Process and Activities, People, Technology, and Other Fixed Assets. This guidance within the DHS EA will provide specific DHS IT programs with a starting point for applying the Performance Reference Model within their Exhibit 300 submissions to OMB.

Support of E-Government Initiatives

The Target EA and Transition Strategy identified several opportunities to leverage on-going e-Government initiatives. As you may be aware, the Department is currently the managing partner for the Disaster Management and Safecom e-Gov initiatives. The Department is also actively participating in six additional e-gov initiatives. For example, there are three major organizations within the department that provide grants to state, local, private industry, academia, and individuals for a variety of reasons that participate in the e-Grants effort. We will be looking more closely at this mode of delivery and how it may leveraged into the EA program.

Finally, the target EA identifies a concept for homeland security information sharing and knowledge flow - the Homeland Security Information Sharing Architecture - based on a concept of Communities of Interest adopted from the intelligence community. Information sharing with state, local, tribal, and other federal government entities is a critical function of DHS, both as a source of information and as the "first responders" to an incident. Implementation of this information sharing architecture will provide value to homeland security community by driving results and productivity through effective information sharing.

In addition to the initiatives for which DHS has the lead responsibility, we expect to be a major contributing player or user of several others. We are committed to transitioning to projects such as e-Authentication, e-Clearance, e-Payroll, e-Travel, and HR Integration. We are actively gaining more knowledge about these initiatives so that our role in supporting them and their particular timelines and capabilities can be integrated seamlessly into our target and transition strategy.

Overview of The EA Plan

Our EA consists of four parts: an “As-Is” architecture characterization, a Business Model, a Target Architecture, and a Transition Strategy for migrating from the As-Is to the Target state.

As-Is Architectural Characterization

The As-Is or baseline architectural characterization describes the DHS enterprise from an IT perspective, and provides a reference point for the development of the target EA and transition planning. The scope of the work was intended to present a high-level assessment of readily available EA-oriented information. It is neither an operational audit, nor is it intended to be a detailed inventory of activities, data entities, applications, locations, or IT elements. Further analysis and refinement is required to provide that level of detail.

The baseline characterization looked at the business activities, data, applications, and IT currently in use by legacy agencies. Also included within the characterization is a view of the DHS FY 2004 major O Ma B exhibits 300. Some high-level observations:

- The current state of DHS architectural artifacts does not lend itself to a full operational audit. Current EA artifacts were developed while organizations were part of their legacy agencies, prior to DHS’ operational start in March 2003. As a result, there are inconsistencies in structure across the legacy EA artifacts that require further definition.
- Considerable overlap exists in business activities among the legacy agencies. Legacy agencies were found to have redundancies in several business activities (e.g., human resources, financial management, procurement, and some mission-specific areas).
- A standard definition of the types of high-level entities (data objects) required to support missions was not uniformly available from all legacy agencies. Data entities (such as “person”) may be defined as a “baggage screener” or a “passenger screener” entering the country, whereas a “document” category may be defined as a “manifest,” “permit,” or “certificate.”
- DHS has over 300 IT applications that are back-office in nature and perform functions such as budgeting, financial management, recruiting, and human resource management.
- DHS has in excess of 1,000 servers and 1,000 various telecommunications circuits clustered throughout the United States and international countries.
- DHS initiatives (OMB Exhibits 300) have significant overlap. Fourteen initiatives were identified, for example, that have a primary emphasis on supporting various credentialing activities.

- Thirty-four initiatives are aligned to at least one e-Government initiative or could use the new General Services Administration (GSA) Smart Buy program.
- The existing DHS Technical Reference Model (TRM) document was incomplete in that it did not adequately address how to provide a common DHS IT standards profile. It also did not give sufficient detail to allow the mapping required to respond to future OMB requirements.

Business Model

The Business Model is the foundation of the EA. It serves as the “business view” of the activities performed by the homeland security enterprise. The homeland security enterprise is defined as DHS, as well as the homeland security functions performed by other entities (state, local, and other Federal) related to securing the homeland.

The business model lists activities and describes these activities to a level of detail that permits an understanding of the data necessary to perform each activity, the system capabilities needed to perform the activities, and the IT to support the capabilities. Hence, the business model “bridges the gap” between the mission and the information systems and underlying infrastructure that support that mission. It was the foundation for the development of a business-driven target EA. The Business Model also provides a framework to identify business outcomes and performance measures and the resources necessary to achieve desired outcomes.

Our Business Model describes the mission, organizational structures, business activities, user classes, and work locations. Documenting our business activities enabled us to identify common activities that can be automated in the optimal target EA and subsequently provided to many users. It comprises several different elements:

- **Value Chain.** A holistic view of business activities across the enterprise, showing high-level business functions that are core to mission fulfillment and that add value to the services provided by the enterprise. The value chain cuts across organizational boundaries.
- **Business Activities.** Decompositions of the high-level business functions independent of the performing organization. Business activities are identified by an appropriate name, which is descriptive and conveys the meaning of the activity, and a textual definition.
- **Performing Organization.** The organizational entities responsible for performing business activities.
- **Workplace Environments.** Descriptions of the actual physical environments where activities are performed. This characterization aids in determining the potential technologies needed to support the automation of the business activity.
- **Workzones.** Physical, geographic locations at which an activity is performed. The four workzones are:
 - **Pushed-back Border** – Activities performed outside the traditional borders of the U.S. This could include activities such as pre-screening passengers or refugee processing.
 - **International Space** – Activities performed in traditional “international” space, also known as international waters or international air space.

- At the Border – Activities performed at traditional U.S. borders. This would include activities such as patrolling the borders (both land and sea), performing inspections on people and goods, etc.
- In the Interior – Activities performed within the traditional U.S. borders.
- Business Scenarios. Key value streams of activities (with clear outcomes) that demonstrate and validate the relationship between activities, the value chain, programmatic and national strategies, and performance outcomes.

Target Enterprise Architecture

The target EA comprises the data, applications, and technology architectures. Although the target will evolve over time, it has been constructed to enable quick and efficient business change by leveraging current best practices in service-oriented and component-based architectures.

To reduce cost and risk, this EA relies on state-of-the-art IT concepts focused on reusable common IT assets, repeatable patterns, and modularity. By designing reuse into the architecture, the cost of meeting new requirements will be reduced. By utilizing repeatable patterns, the risk in developing new IT assets will be minimized. This will, in turn, reduce the schedule and performance risk for IT projects. The modular concepts embedded in the architecture will allow the enterprise to be more agile in responding to change. IT applications can be assembled from a set of existing “building blocks” rather than having to be built as new large-scale IT development efforts.

Data Architecture. DHS requires an efficient means of handling data across the Department, both for normal business purposes, and to enable DHS and other entities to share timely, accurate, accessible, and reusable information. The data architecture was driven by and developed in conjunction with the Business Model, using a parallel decomposition approach. The data architecture identifies the enterprise-wide data necessary to support business activities, without regard to organizational or procedural boundaries. It focuses on answering the question: “What information is needed to accomplish this activity?” The data architecture was designed to satisfy two main objectives: to provide common vocabulary across the enterprise and to provide understanding of the fundamental (data) structure of the enterprise. It consists of a list of subject areas (with definitions), data objects (with definitions, key characteristics, and important relationships), a high-level Entity Relationship Diagram, and a data-usage matrix, referred to as the CURE Matrix.

Application Architecture. The purpose of the target application architecture was to develop an easily understood picture of the type of application systems that would satisfy the Department’s business needs. The target application architecture defines the “to be built” applications and components, describing the required functions and capabilities to support business needs. It is based on commercial best practices and a new paradigm promoted by the Office of Management and Budget (OMB) and the Federal Chief Information Officer Council: Service/Component-Based Architecture.

Service/Component-Based Architecture divides the functionality of the applications into the services provided. Services, in turn, are implemented by reusable software components. Construction of applications consists of assembling components into a meaningful whole that satisfies a set of business needs. The concept of monolithic applications that provide all functionality in a particular area (of which each individual might use only a small portion) is dispensed with in favor of a flexible “virtual application” that brings together the services provided by the components that are applicable to the individual’s task. An application thus becomes the software to manage the workflow associated with the particular task. This paradigm has many advantages. Among these advantages are reduced user training, easily modified applications (plug and play), reuse of components in multiple applications, and better interoperability of applications.

The target application architecture lays the foundation for defining the IT software to be built, assembled, reused, mined, and acquired to provide the tools to conduct normal business operations. It was based upon the activities defined in the business model and data objects defined in the data architecture. It is a notional architecture, meaning it does not attempt to define in detail each application that will be required by the enterprise. Instead, it defines the types of application groups that will be required and the types of software components that each application group will consume.

Technology Architecture. The target technology architecture assists those responsible for delivering and maintaining business systems. It defines the platform upon which all DHS assets will operate. Providing a common platform is critical to achieving the objectives that caused the Department to be created (e.g., information sharing, interoperability, effective communication, etc.). The target technology architecture consists of technology principles; a set of technology patterns; a technical reference model (TRM); and a Standards Profile. The technology patterns are implemented using technology categories that are defined in the TRM. The Standards Profile identifies the acceptable standards, protocols, and products for the categories in the TRM.

Patterns represent industry-accepted solutions to repetitive problems or issues facing IT. The focus of the EA is on architecture-level patterns. A set of drivers (requirements or features) is applied to the applications to allow a mapping of the applications and components to appropriate technology patterns. Technology categories are then applied to the patterns. This provides the basis for developing the Standards Profile for those categories implied by the patterns.

The DHS TRM describes the technology platform upon which the application and other architectures rest. It provides a common conceptual framework that assists in coordinating the acquisition, development, operation, and capitalization of IT assets. It provides a common structure and vocabulary for describing DHS IT at all organizational levels and in all environments. The TRM establishes the basic guidance necessary to ensure that proposed IT solutions are compliant with the intent of the EA. Finally, the TRM includes communication and interoperability categories that provide the technical basis for interfacing with state, local, and other government agencies. The goals of the TRM and DHS standards profile are as follows:

- Promote vendor independence through the use of standards-based products and interchangeable services and components.

- Improve interoperability, reuse, and information sharing across operational entities.
- Improve operational effectiveness and efficiency through the use of common concepts and tools.
- Improve security through the identification of common security services and standards.
- Improve development and integration efficiency and responsiveness through the identification of a common infrastructure for applications.
- Improve development and integration quality through implementation of a Department-wide systems assurance program.

Information Sharing Architecture. One of the fundamental drivers in the establishment of DHS was the need to share information in a timely manner among the intelligence, law enforcement, emergency management, responder, and other communities. DHS has requirements to share and access information at many different levels. Above all, it needs the capability to provide data to all users that have a need for it—to exchange that data with other Federal agencies (horizontal sharing), and with state, local, private sector, and tribal governments (vertical sharing), as well as with foreign governments. Information sharing, whether horizontal or vertical, generally refers to the ability to access and share critical information with key business partners. The information sharing architectural description within the target describes the most common models for information sharing: push, pull, query/response, and publish/subscribe. Depending on the type of information, its urgency, the consumer, and the available technology, DHS may rely on any or all of these models.

Transition Strategy

While our first step in meeting the challenges that face IT in helping the Department meet its mission and objectives has been accomplished—producing a business-driven Target EA—the second step is actually implementing that target. Our Transition Strategy guides us as we make decisions about our current environment so that we can, project by project, realize the target. The strategy identifies objectives that will be met through the implementation of conceptual projects. Those objectives are to unify the DHS infrastructure, address immediate critical mission needs, address mandated project dates, optimize corporate solutions, and provide new and improved mission capabilities.

Taken together, the target EA and transition strategy describe an IT environment that is vastly different from the one that exists today, an IT environment that:

- Captures data at its source, avoiding costly multiple data capture.
- Allows data access by multiple applications, so that data once collected is available to all decision makers.
- Leverages information sources that decision makers might not normally have had access to.

The EA also contributes to improved data sharing capabilities. It helps us identify the data requirements of each business activity and for each relevant stakeholder. Through the EA

planning process it is possible to identify where data actually resides, who uses the data, where the data is used, and when the data must be available. The result is enhanced sharing capabilities by virtue of developing IT systems that collect data necessary to support business activities only once, but make the data available many times over to support other homeland security business activities.

The relevance of the our Transition Strategy is that we are using it today, right now, to make decisions about our IT investments. The strategy guides us as we decide to initiate new projects, modify existing applications, consolidate many investments into fewer, build new capabilities, then field improved information systems, or deploy enabling technology infrastructure to better support mission performance. The most immediate impact of the Transition Strategy is its use in deciding what projects to initiate or continue in FY04, most significantly which existing investments must be considered for consolidation to better align existing resources to new mission requirements, and save significant resources—financial and human—with the elimination of redundant investments. Each conceptual project in our Strategy identifies existing investments that are consuming financial and human resources today that will be considered for consolidation or elimination as the capability to meet that business need is designed, built, and fielded.

Our Transition Strategy is the foundation of a more detailed transition plan that will identify more concrete steps for moving to the target EA. As we refine our target and the transition strategy itself, we will have a more significant impact on the budget formulation processes and the requests we make for IT investments for FY06 and beyond.

Challenges

It would be easy to rest on the laurels of what we've accomplished in such a short period of time. It was a Herculean effort accomplished in a very short period of time and has resulted in an actionable strategy for moving forward. In reality, however, we have only just begun the journey to get from where we are today to where we need to be tomorrow and into the future.

DHS faces a number of challenges in building upon the success of our initial EA effort. First, we need to move DHS culture closer to a "One DHS / One Enterprise Architecture" culture and further away from "stove piped" legacy thinking by further engaging our business units in the maturation of this EA. Second, as we begin to implement the target EA, we need to re-orient and potentially redirect some current IT investments. This will be a challenge as we move from a culture of "ownership" to one of "stewardship" that requires business users to share and re-use IT assets to the maximum extent practicable. Third, as we re-engineer our business processes, we need to better align our capital assets (human, real, IT) to meet the needs of those improved processes. Finally, we need to implement and embrace a disciplined, enterprise-wide architecture governance process. This process will lead to optimal IT investment decisions across the DHS enterprise and successful IT implementations. I am confident that as we move forward, and with your guidance and assistance, we can overcome these challenges, and in the process, become a model organization for business and IT transformation.

Finally, EA planning is being performed at the Department level. This approach will facilitate the optimal use of IT resources by applying common architecture principles and establishing a

common architectural framework to ensure uniformity and standardization when migrating and integrating IT investments. A collaborative approach will ensure that overlapping business processes and data needs are identified, and that applications and IT supporting those applications will not duplicate each other. It will also ensure that the EA addresses the unique aspects and business missions of each of those organizations. Our challenge is that it requires significant input, dedication of resources, and the close collaboration of the DHS Directorates and organizational elements to develop a single DHS-wide EA. Concurrently, many of the legacy agencies now within DHS have conducted EA planning projects and are maintaining mature EA support structures. We must find the right balance between leveraging what we have, and creating a new, single, DHS-wide framework.

Next Steps

While the development of our EA plan is an important first step, it is just that, a first step. The value of an EA is in its ability to improve IT investments and resources management in a manner that advances DHS mission performance in both the short and long term. In the near term:

- **We are using the results of our EA effort today to support our immediate investment decisions.** We are doing this by aligning and integrating our current investments to leverage our investment review process to ensure solid enterprise architecture-based justifications for our investments.
- We will begin implementing “**quick hit**” items – beneficial modest scale investments that will quickly deliver needed capabilities consistent with the target architecture.
- We are evaluating existing programs against the EA and consolidating investments where there are **areas of overlap and duplication.**

As we start the hard work of evolving our EA architecture beyond the conceptual level, we will begin to make direct links between specific detailed target architecture elements and specific IT projects. This will also allow us to mature the transition strategy into a detailed, specific project plan for evolving to the target architecture. In addition, we will begin to put in place the necessary processes to ensure that business and technology strategies and investments remain aligned over time to meet DHS’ mission priorities. These specific next steps will ensure that we continue along our EA based roadmap and that we are ultimately successful in transforming DHS to optimally meet our critical mission.

Thank you, Mr. Chairman, for this opportunity to discuss the DHS EA.

Attachment A
DHS Enterprise Architecture Participants and Support Contractors

DHS Headquarters

George Brundage, Catherine Santana, Charles Thomas, Amy Wheelock, Ron Williams

Border and Transportation Security Directorate

Bureau of Immigration and Customs Enforcement

Glenn Norton, Paul Rosenberg Mike Nicholson

Bureau of Customs and Border Protection

Rick Alcocer, Phil Cullens, James Jeffers, Shenell Jennings, Brian Nicholas, Will Peters, Brenda Stealing, William Tyree

Federal Law Enforcement Training Center

Robert Crouch, William Dooley, Ned Futoran, Sandra Peavy

Transportation Security Administration

Mark Emery, Jonathan Houk

Bureau of Citizenship and Immigration Services

Patty Cogswell

Emergency Preparedness and Response Directorate

Tom Brace, Jack Fox

Information Assurance and Infrastructure Production Directorate

Tim Daniel, Keith Herrington

Science and Technology Directorate

Parney Albright, David Boyd, Maureen McCarthy, Robert Shepherd

United States Coast Guard

Bradford Eyre, Jack Green, Ron Hewitt, David McLeish

United States Secret Service

William Cachinero, Ken Gunderson, John Gutmied, Gregg James, Damian Kokinda, Greg Lydon, Doug Schraeder

DHS Enterprise Architecture Support Team

Science Applications International Corporation (SAIC)

High Performance Technologies, Inc. (HPTi)

Everware