

# Integrated United States Air Surveillance Governance Report

Final Report July 7, 2010



**Reviewed by the  
Departments and Agencies for the  
Next Generation Air Transportation System**

Reviewed & Approved.  
Joint Planning and Development Office

Dr. Karlin Toner

Reviewed & Not Approved.

Department of Defense

*Note: DoD does not approve this report. DoD concerns and reservations are discussed in the Preface.*

Reviewed & Approved.  
Department of Commerce/National Oceanic  
Oceanic and Atmospheric Administration

Mr. Donald Berchhoff

Reviewed & Approved.  
Department of Homeland Security

Mr. Kevin Kirsch

Reviewed & Approved.  
Department of Transportation/  
Federal Aviation Administration

Mr. James H. Williams

Reviewed & Approved.  
Office of the Director for National Intelligence

Mr. Steven Cantrell

  
\_\_\_\_\_  
Dr. Karlin Toner  
Director, Joint Planning and  
Development Office

## PREFACE

The IS Governance Task Force (Task Force) initiated its work in September 2009 for presentation to the Senior Policy Committee in July 2010. While the Task Force was deliberating however, a comprehensive activity was initiated to achieve a whole-of-government approach to Air Domain Awareness (ADA), which encompasses air surveillance services and cross-agency information sharing. The ADA initiative also recognized the need for an interagency governance mechanism for ADA. Senior advisors for ADA and Integrated Surveillance governance from DHS, DoD, DOC and FAA collaborated to ensure that Integrated Surveillance efforts continue moving forward while the ADA work coalesced.

On June 8, 2010 the IS Governance Task Force report was circulated for formal coordination to the NextGen partner agencies in preparation for presentation to the Senior Policy Committee. The IS Governance Task Force recommendation recognizes the understanding that when the ADA effort is sufficiently mature, the Integrated Surveillance governance organization will either be incorporated as appropriate into the ADA governance structure, or the Integrated Surveillance governance organization will expand to incorporate ADA.

Before coordination of the IS Governance Task Force report could be completed, however, Department/Agency leaders at the July 2010 Air Domain Awareness (ADA) Summit decided that, rather than establish a cabinet-level oversight board, the emerging ADA governance mechanism should instead leverage the existing National Security Staff interagency policy coordinating processes. The NSS process includes Assistant Secretary, Deputy Secretary, and Secretary-level coordinating committees. In subsequent conversation, the National Security Staff's Senior Director for Transborder Security proposed that the Integrated Surveillance governance mechanism also leverage the existing NSS processes for general oversight, and to address issues that cannot be resolved at lower levels.

DoD can not approve the IS Governance report as written. The DoD is unresolved on the timing of transferring IS efforts under the auspices of the JPDO to the anticipated Air Domain Awareness Organization. If an ISSO were to be created, DoD has reservations concerning the size of the ISSO, and the level of decision making authority. Also, while the proposed interagency organization can be created to facilitate collaboration and promote efficiencies and information sharing; absent new legislation or an Executive Order, the proposed interagency organization would not have any authority to govern or bind a federal agency. Further, providing support in the form of funding or manpower to an organization that has no clear organic legislation or budget is fundamentally problematic. The DoD support to the interagency organization proposed by this report exceeds the level of support that DoD is authorized to provide by the Century of Aviation Act and Executive Order 13479. While DoD may not staff or fund the proposed interagency organization, DoD employees or contractors may work, in coordination with partner organizations, to further DoD's mission. Although the DoD cannot endorse this document without reservations, it contains some valuable information for consideration, and is published with the aforementioned reservations.

On July 26, 2010, the NextGen SPC, chaired by DOT Secretary LaHood, was briefed on the current surveillance challenges, the progress made in resolving these challenges, and

recommendations for further progress. Specifically the interagency team recommended that partner departments and agencies:

- Integrate the IS Governance Recommendations with recent guidance from the National Security Staff, and execute a memorandum of agreement (MOA) that allows IS work to go forward
- Identify executives to monitor progress and remove barriers
- Identify individuals to perform the work outlined in the IS Governance Report.

The SPC recognized the need for long-term integration and alignment of surveillance capabilities, and directed staff to continue working towards this end. The SPC recognized DHS's executive leadership role, and the need for transition of oversight to the National Security Staff. The SPC also asked staff to identify earlier capabilities that could be in place in a year.

Whether addressing air surveillance, air domain awareness, or all transportation domain awareness, effective interagency governance will be critical if taxpayer investments are to be optimized and safety and security risks minimized. Effective interagency cooperation does not come naturally or easily. While the specific organizational elements recommended in Section 2.3 of this report may be overtaken by events, the underlying research, analysis, and conclusions about the characteristics of an effective cross-boundary governance mechanism remain valid, and can serve as a baseline of knowledge for development of other interagency governance structures.

## Table of Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>REPORT .....</b>	<b>4</b>
1.0 Background and Definitions .....	4
2.0 Organization and Operation of the Interagency IS Governance Task Force .....	8
2.1 Task Force Participants .....	9
2.2 Methodology .....	9
2.3 Recommended Approach to IS Governance and Rationale .....	10
2.3.1 Values, Scope, and Key Characteristics.....	10
2.3.2 Recommended IS Governance Entity .....	14
2.3.3 External Factors Recommended for Success .....	22
2.3.4 Transition Recommendation .....	23
2.3.5 Relationships to Complementary Activities.....	24
DOCUMENT REVISION HISTORY .....	30
<b>APPENDIX A.....</b>	<b>1</b>

## **EXECUTIVE SUMMARY**

Multiple federal departments and agencies have need for aviation surveillance information and have existing infrastructure, services and programs to meet those needs: the Federal Aviation Administration (FAA) for administering the aviation transportation system<sup>1</sup> and air security, the Department of Homeland Security (DHS) for airborne and airport security, and the Department of Defense (DoD) for air defense. The Department of Commerce (DOC) provides hazardous weather information and forecasts to aid agencies in situational awareness and in the use of aviation surveillance information and will likely use data from non-DOC systems with weather surveillance capabilities. The overlapping roles, responsibilities, authorities, and capabilities of the air surveillance mission partners have led to cross-dependencies among the agencies in terms of surveillance system ownership and use of the information produced by these systems, as well as an operational need for timely surveillance information sharing across agencies. However, there is no current institutional mechanism for reconciling these overlaps and coordinating policy, requirements, funding, plans or operations of the nation's aviation transportation system surveillance assets.

Federal departments and agencies with aviation and air defense missions (hereafter the "IS departments and agencies"), specifically the DOC, DoD, DHS, Department of Transportation (DOT), and Director of the Office of National Intelligence (ODNI), came together in the fall of 2009 and established an interagency Integrated US Air Surveillance<sup>2</sup> (IS) Governance Task Force. They charged the Task Force with examining whether and how IS departments and agencies might establish a governance mechanism to manage IS services in a manner that improves safety and efficiency of the air transportation system, and contributes positively to the national defense and homeland security. The Task Force acknowledges that establishment of IS Governance is proceeding as an independent activity in parallel with the broader interagency activity to develop governance for Air Domain Awareness (ADA). It is understood that in the future when ADA is better understood, the IS governance organization will either expand to incorporate ADA governance or the IS Governance organization will be incorporated as appropriate into the ADA structure.

In the following report, the IS Governance Task Force summarizes the results of a best practices analysis of other interagency governance constructs of analogous scope and mission to that

---

<sup>1</sup> Aviation Transportation System is US airspace (the NAS), all manned and unmanned aircraft operating in that airspace, all US aviation operators, airports, airfields, air navigation services, and related infrastructure, and all aviation-related industry.

<sup>2</sup> Integrated US Aviation Transportation System Surveillance is the integration of information from cooperative and non-cooperative surveillance systems to create a user-defined operational picture (from common information) of real or near-real-time situation for safety, security, and efficiency, within the scope of the US Aviation Transportation System.

presented by IS, and uses that analysis to inform its recommendations for IS governance. The report then states the Task Force's recommended organization for IS governance.

The Task Force recommends that an enduring interagency organization be established for collaborative management of IS services. It should be based on a consortium, rather than a directive executive model. At the highest level, agency differences and disputes not resolved by the IS organization at a lower level may be mediated by a Cabinet-level Senior Surveillance Oversight (SSO) function, which would operate in a manner consistent with the pending ADA governance structure. In the interim, until a final SSO organization is decided, the Task Force recommends that the existing NextGen Senior Policy Committee<sup>3</sup> serve in the role of SSO. A senior-level board of IS department/agency executives--the Integrated Surveillance Senior Action Committee (ISSAC)--would provide overall IS management and policy direction. IS technical work would be performed by a robust network of ISSAC subcommittees and work groups, facilitated and supported by an independent, honest-broker Integrated Surveillance Support Office (ISSO). The ISSO would be funded jointly by the IS partner departments and agencies, and resourced additionally with technical personnel detailed by the partners.

Participants in interagency IS work would strive for consensus decisions. The technical support organization would attempt to mediate differences among department/agency representatives at the working group level. Intractable differences would be elevated to the ISSAC for mediation; those still unresolved could progress upward for mediation by the Cabinet-level SSO. If still unresolved, any member of the SSO including the Chair could seek resolution through the National Security Staff (NSS).

The Task Force recommends that the IS governance organization be incorporated in a Presidential Executive Order or Directive, as part of a more comprehensive directive establishing ADA governance or if necessary, directed solely to IS governance. The Task Force also encourages department/agency senior officials to be actively engaged in IS matters, and recommends that senior Office of Management and Budget (OMB) officials remain aware of IS planning by observing ISSAC deliberations.

In summary, the Task Force recommends that, pending establishment of ADA governance, the SPC take the following steps to implement an interim IS governance organization so that work can proceed immediately on interagency planning and implementation of IS services:

- Provide staff and resources for the ISSAC and ISSO structure under SPC policy guidance and oversight;

---

<sup>3</sup> "Vision 100" Section 710, 49 USC 40101 establishes the Senior Policy Committee, chaired by the Secretary of Transportation, to work with the Joint Planning and Development office (JPDO). The SPC is composed of the Administrators of FAA and NASA, the Secretaries of the Departments of Commerce, Defense, and Homeland Security, and the Director of the White House Office of Science and Technology Policy. ODNI was added later to the SPC because of their equities in IS.

- Direct the ISSAC and ISSO to begin needed system engineering efforts;
- Inform the cognizant National Security Staff of these interim steps to advance the national integrated surveillance capability; and
- Direct IS departments to finalize and sign an interagency IS governance MOA to institutionalize their shared commitment.

# REPORT

## 1.0 Background and Definitions

Multiple departments and agencies have a need for Aviation Transportation System surveillance information and have existing resources and planned programs to meet their mission needs: the FAA for administering the National Airspace System (NAS) and air security, DHS for airborne and airport security, and DoD for air defense. DOC provides hazardous weather information and forecasts to aid agencies in situational awareness and in the use of aviation surveillance information and will likely use data from non-DOC systems with weather surveillance capabilities.

The overlapping roles, responsibilities, authorities, and capabilities of the surveillance mission partners have led to cross-dependencies among the agencies in terms of surveillance system ownership and use of the information produced by these systems, as well as an operational need for timely surveillance information sharing across agencies. However, there is no current institutional mechanism for reconciling these overlaps and coordinating policy, requirements, funding, plans or operations of the nation's aviation transportation system surveillance assets.

Within this context, establishing legislation<sup>4</sup> charges the interagency Joint Planning and Development Office (JPDO) with the responsibility of creating and carrying out an integrated plan for the Next Generation (NextGen) Air Transportation System that, among other characteristics:

“(2) take[s] advantage of data from emerging ground-based and space-based communications, navigation, and surveillance technologies;

(3) integrate[s] data streams from multiple agencies and sources to enable situational awareness and seamless global operations for all appropriate users of the system, including users responsible for civil aviation, homeland security, and national security; [and]

(4) leverage[s] investments in civil aviation, homeland security, and national security and build[s] upon current air traffic management and infrastructure initiatives to meet system performance requirements for all system users....”

Executive Order 13479, Section 4 (a)(ii) charges DoD with the responsibility of supporting the DOT in its NextGen mission by “furnishing, as appropriate, data streams to integrate national defense capabilities of the United States civil and military systems relating to the national air transportation system, and coordinating the development of requirements and capabilities to address tracking and other activities relating to non-cooperative aircraft in consultation with the Secretary of Homeland Security, as appropriate.”

---

<sup>4</sup> Vision 100 – Century of Aviation Reauthorization Act (Pub. L. 108-176), 49 USC 40101 note.

Based on Air Domain elements of NSPD-47/HSPD 16 as expanded upon in the follow-on NSAS Air Domain Surveillance and Intelligence Integration Plan (NSAS), beginning in 2007 DHS and DoD co-hosted a series of Summits to consider department roles and responsibilities and governance of air surveillance. At the same time in mid-2007, in furtherance of its legislated mission the JPDO established the NextGen Integrated Surveillance Study Team (ISST) as an interagency group. On November 21, 2008, representatives of the JPDO partner agencies approved the Final Recommendations of the ISST. Key findings of the ISST include the following:

- There are known organizational barriers to achieving NextGen surveillance objectives that must be addressed before any technical approaches can be successfully evaluated, selected, and implemented.
- There is no institutional mechanism to oversee and coordinate surveillance capabilities across all agencies, nor is there a mechanism in place to synchronize and arbitrate agency efforts to establish an Integrated Surveillance capability.
- There are gaps between NextGen needs and planned surveillance capabilities due to sensor coverage and detection characteristics; data correlation and fusion; network architecture and connectivity; interagency surveillance information sharing and collaboration; and ability to address the spectrum of multi-agency information needs. There is no consensus among the agencies that participated in the ISST study regarding the degree to which these gaps cause near-term operational risks.
- No concept of operations exists that covers the scope of integrated surveillance. Surveillance is currently characterized by each individual agency focusing only on its own operational mission needs.
- Limited capabilities exist for the timely sharing of surveillance information across all stakeholders, which also affects the coordination of responses to detected events.
- There are opportunities to leverage future technologies and other capabilities across agencies to achieve synergy in Integrated Surveillance.

The ISST recommended that IS departments and agencies<sup>5</sup> undertake to:

- Determine and establish a formal, institutionalized interagency mechanism for responsibility, management, and ownership for elements of integrated surveillance (to include funding)
- Develop a concept of operations for NextGen Integrated Surveillance

---

<sup>5</sup> The Department of Defense (DoD), the Department of Commerce (DOC), the Department of Homeland Security (DHS), the Federal Aviation Administration (FAA), and the Office of the Director of National Intelligence (ODNI).

- Develop an interagency Integrated Surveillance architecture to support operational, system, technical, and investment decisions
- Develop and implement an Aviation Surveillance Information Network strategy
- Develop and execute an interagency Integrated Surveillance implementation plan
- Use demonstrations and experiments to mature and field early versions of Integrated Surveillance capabilities.

At the third DHS/DoD hosted Summit on December 2, 2008, surveillance partner representatives recommended that the JPDO request the SPC to meet and accept interim oversight of the integrated surveillance aspects of ADA, including development of an IS ConOps, joint enterprise architecture, and recommendation for long-term governance. These three products would then go before a NSC/HSC Deputies Committee (likely by that point a NSC Deputies Committee) for ratification or revision, particularly the decision concerning long-term governance. In 2009, DHS/DoD co-hosted the ADA Summit and activity began for consideration of a governance structure for Air Domain Awareness, work that is now progressing in parallel with IS governance which is the subject of this report.

In a meeting on January 7, 2009, the SPC accepted the interim IS oversight role recommended by the third interagency Surveillance Summit, and directed the JPDO to coordinate work on the IS ConOps, joint enterprise architecture, and recommendation for long-term governance. On the basis of the SPC's January 7 directive, the JPDO in September 2009 invited senior representatives of the IS departments and agencies to engage in a collaborative activity to implement the first ISST recommendation: "Determine and establish a formal, institutionalized interagency mechanism for responsibility, management, and ownership for elements of integrated surveillance (to include funding)." This report documents the methodology and results of that analysis and provides recommendations for Interagency IS Governance.

The Senior Policy Committee (SPC) also tasked the IS agencies to develop an IS ConOps and IS Enterprise Architecture (IS EA). In keeping with the four month target timeframe set by the SPC, a cross-agency team delivered the draft IS ConOps Version 3.0 to the JPDO Board in June 2009 and, as intended, provided a foundation for follow-on development of the IS EA. The IS EA task was intended to influence funding decisions for Fiscal Years 2012 – 2016. Formal approval by the IS partners has not been achieved, and the IS ConOps and IS EA remain in draft status.

The Draft IS ConOps targets a need for national IS common services to be able to:

- automatically confirm when they are looking at the same track and its associated information;
- ability to track non-cooperative targets;
- access pre-flight information in a timely manner;

- receive automated, in-flight updates on changes in key flight characteristics; and
- operate with increased confidence as a result of enhanced and shared track monitoring.

The Draft IS EA Results and Recommendations Report (see fn. 15) endorsed desired capabilities identified in the IS ConOps and added some additional significant needs:

- interagency IS coverage;
- a formal interagency coordination process for research and development, requirements development and validation, and acquisition of IS capability; and
- closing of mission gaps in implementing aviation security risk management.

Given the challenges for reaching cross-agency consensus on difficult IS issues, implementation of an IS governance structure capable of mediating among diverse agency needs and perspectives will be critical to cooperatively advancing work on the IS Con Ops and IS EA.

The following definitions are used in this Report (except where indicated, all definitions are derived from the ISST Report):

**Air Domain:** The global airspace, including domestic, international, and foreign airspace, as well as all manned and unmanned aircraft operating, and people and cargo present in that airspace, and all aviation-related infrastructures.<sup>6</sup>

**Air Domain Awareness:** The effective understanding of threats associated with the Air Domain that could impact the security, safety, or economy of the United States.<sup>7</sup>

**Air Surveillance System:** The sensors, automation systems, and data distribution associated with the air domain.

**Aviation Transportation System:** U.S. airspace, all manned and unmanned aircraft operating in that airspace, all U.S. aviation operators, airports, airfields, air navigation services, and related infrastructure, and all aviation-related industry.<sup>8</sup>

**Enterprise Architecture (Integrated Surveillance):** The body of data and products organized in such a way to decompose, define and relate the enterprise-level operational

---

<sup>6</sup> NSPD-47/HSPD-16.

<sup>7</sup> NSAS Air Domain Surveillance and Intelligence Integration Plan, March 26, 2007.

<sup>8</sup> NSPD-47/HSPD-16.

activities, capabilities, information exchange requirements, services, and performance requirements needed to achieve the IS goals and objectives.<sup>9</sup>

**Integrated US Air Surveillance (IS):** The integration of information from cooperative and non-cooperative surveillance systems to create a user-defined operational picture (from common information) of real or near-real time situation for safety, security, and efficiency within the scope of the Aviation Transportation System.

**Integrated Surveillance Services:** Surveillance sensors and their output, and any data or information helpful for interpreting that output, required by or useful to more than one integrated surveillance mission partner."<sup>10</sup>

**JPDO Government Partners:** DoD, DHS, DOT/FAA, DOC, NASA, OSTP, ODNI.

**NextGen:** Next Generation Air Transportation System (see Public Law 108-176, "The Vision 100 - Century of Aviation Reauthorization Act.")

**Non-Cooperative Surveillance:** Employs a number of techniques to detect and/or identify an object of interest; does not require participation from the airborne object.<sup>11</sup>

**Surveillance:** The ability to obtain or derive the position, vector and, if available, the identity and flight path intent, of an object within the Air Domain, or about to enter the Air Domain (also referred to as air surveillance).<sup>12</sup>

**Surveillance Mission Partners:** DoD, DHS, DOT/FAA, DOC (also referred to as mission partners).

**Weather Surveillance:** The means, through human observation and automated sensors, to measure the characteristics of the atmosphere. It can be done using in-situ instruments or remotely by space-, air-, and land-based systems, including on-board sensors, radar, and satellite technologies.

## **2.0 Organization and Operation of the Interagency IS Governance Task Force**

---

<sup>9</sup> Interagency Architecture and Engineering Division.

<sup>10</sup> IS Governance Task Force.

<sup>11</sup> IS Governance Task Force.

<sup>12</sup> NSAS Action Items 95 and 98.

## ***2.1 Task Force Participants.***

IS departments and agencies participated in work of the Task Force, Chaired by Peggy Gervasi, JPDO Director, Strategic Interagency Initiatives, through Senior Advisors and Agency Leads. The Senior Advisors provided strategic and policy guidance, and validated study direction and products. Senior Advisors, by agency, were:

Don Berchoff, Director, Office of Science and Technology, National Weather Service,  
Department of Commerce  
Col David Jones, Chief, NextGen Lead Service Office, Department of Defense  
Kevin Kirsch, Director, Office of Special Programs, Department of Homeland Security  
James Williams, Director, Systems Engineering and Safety, Federal Aviation  
Administration  
Steven Cantrell, Acting Assistant Deputy Director of National Intelligence Global  
Maritime and Air Intelligence Integration Office of the Director of National Intelligence  
Charles A. Leader, Director, Joint Planning and Development Office.

The Agency Leads engaged in expert analysis of exemplars, identified governance best practices, and developed IS governance consensus principles and operating construct. Leads by agency were:

Robert Saffle and Judson Stailey, Department of Commerce  
Lt Col Philip Basso, Department of Defense  
Andrew Florell, Cdr. Edward Sheppard, Richard Rogers, and Robin Dooley, Department  
of Homeland Security  
Donald Frenya, David Olsen and EJ Beaulieu, Federal Aviation Administration  
Josh Holtzman and Mark McDonal, Office of the Director of National Intelligence  
Doug Arbuckle, Joint Planning and Development Office.

## ***2.2 Methodology***

The IS Governance Task Force deliberations proceeded in two phases.

First, the Task Force considered whether there were existing interagency entities that might be suitable, capable and acceptable to IS agencies to take on the responsibility of IS interagency governance. No such organizations were identified.

During the second phase of deliberations, the Task Force developed a recommended construct for a dedicated entity to assume the responsibility of governing collaboration among IS agencies about services.

The Task Force identified four ongoing interagency collaborative activities (exemplars) having comparable missions and scope to that contemplated by the IS agencies, to examine and analyze for best governance practices, effectiveness, and lessons learned. In accordance with ISST recommendations, exemplars were selected that exhibited both the consortium (requiring

interagency agreement on a common architecture and collaborative management) and executive (designation of a lead agency as single entity responsible and accountable for all integration issues) approaches to governance. The four exemplars were: Position, Navigation and Timing (PNT) Executive Committee/National Coordination Office; Interdepartment Radio Advisory Committee (IRAC)/National Telecommunications and Information Administration (NTIA/IRAC); National Coordination Office for Health Information Technology (NCOHIT); and Program Manager—Information Sharing Environment (PM-ISE) (partial analysis).

The analysis was conducted through briefings by agency leaders of those exemplars, interviews of non-leadership participants in those exemplars, and literature searches for additional information. The exemplars were specifically evaluated for their effectiveness in synchronizing and arbitrating agency efforts in

- policy development,
- requirements generation,
- technology maturation,
- funding decisions,
- system acquisitions,
- system operations;

and, in holding partners accountable for follow through on joint decisions; and mediating among diverse mission partners.

On the basis of the knowledge gleaned from the exemplars analysis, the Task Force engaged in collaborative discussions to define the values of interagency IS governance, delineate the appropriate scope of services/activities subject to collaborative governance, and agree on key characteristics of a recommended governance entity. The output of those discussions was embodied in the draft recommended governance document included in this Report, and accompanying recommendations for how such a construct could be effectively implemented.

A summary and analysis of the information gathered about each of the four exemplars is Appendix A to this report.

## ***2.3 Recommended Approach to IS Governance and Rationale***

### **2.3.1 Values, Scope, and Key Characteristics**

On the basis of the insights derived from the exemplar analysis, the IS Task Force engaged in collaborative discussions to develop the following best practice values, scope and key characteristics for integrated surveillance governance.

Values. The IS agencies agreed that collaborative management of surveillance services will provide opportunities to:

- Streamline government operations to improve performance and effectiveness;
- Reduce costs and thereby save taxpayer dollars;
- Optimize overall national surveillance outcomes;
- Increase prospects for achieving optimal funding profiles for surveillance programs and projects;
- Improve trust among departments and agencies, and increase willingness to adopt collaborative and joint--as opposed to independent--approaches to managing surveillance services;
- Improve awareness among departments and agencies about ongoing research and development of surveillance technologies, thereby encouraging joint /collective approaches and activities;
- Avoid and remediate gaps and disconnects that lead to miscommunications;
- Develop awareness of common needs and shared urgency that will help drive top-level department and agency management engagement;
- Facilitate development of a common architecture for IS services.

*Scope.* Based on analysis of the ISST, National Strategy for Aviation Security (NSAS) Action Item Reports (*see* footnote 7), the interim draft IS ConOps and interim draft IS Enterprise Architecture Results<sup>13</sup>, the Task Force recommends that the following scope of work be undertaken by the proposed IS governance entity. In general the proposed entity should engage in planning, integrating, and synchronizing agency activities directed toward providing IS services, including providing technical support and mediating differences among partner agencies when necessary. The IS governance entity should at the least:

- Maintain and evolve the Concept of Operations (ConOps);
- Maintain and evolve the interagency architecture<sup>14</sup> to support IS operational, system, technical, and investment decisions;
- Develop, maintain and monitor the execution of an interagency IS implementation plan<sup>15</sup>;
- Synchronize and mediate<sup>16</sup> among diverse IS mission partners for:

---

<sup>13</sup> The draft *Integrated Surveillance Concept of Operations*, Draft V 3.0, submitted to the JPDO Board on June 16, 2009, has not been approved by the agencies. The *Integrated Surveillance Results and Recommendations Report* draft version 0.7 has not been approved by the agencies and will be turned over to the governance body after establishment.

<sup>14</sup> The IS Enterprise Architecture (EA) will decompose, define and relate the enterprise-level operational activities, capabilities, information exchange requirements, services and performance requirements needed to achieve the IS goals and objectives. The IS EA will be used as an analysis and decision support tool to inform interagency investment strategy development, acquisition decisions, research actions and technology demonstrations, and synchronizing IS capability implementation and deployment through federation with agency surveillance architectures.

<sup>15</sup> *See* ADSII Action Item 102, which provided a high level “coordinated air surveillance implementation plan to integrate civil and military surveillance capabilities and recommend solutions for any gaps in aviation security requirements.”

- policy development;
- capability/requirements generation;
- technology maturation;
- funding (fair allocation of costs);
- systems acquisition and operations.

*Key Characteristics.* First, the Task Force recommends that the IS Governance be based on the consortium, and not the executive model. It was noted that organizations operating successfully in the executive model were called upon by others to develop and implement systems, services, and/or capabilities in which they were already predominantly invested, or for which they had unique infrastructure or technical capability. In those cases, it made sense from a technical and financial point of view for other departments and agencies to rely on one, or a few entities to provide services to the others. On the other hand, the consortium model was more suited to groups of departments and agencies already invested in infrastructure and capabilities dedicated to individual agency mission needs, but which would benefit from collaboration, leveraging and improving of those IS services. Whereas the IS agencies each have significant surveillance infrastructures and capabilities already devoted to their own mission needs, it was determined that the consortium model focusing only on collaborative management of those IS services would be the appropriate basic IS construct.

The Task Force also agreed that the IS governance entity should exhibit the following key characteristics, many of which are modeled on the successful NTIA/IRAC example:

- Clearly defined and documented organizational structure;
- Members of the highest level body to provide goals and objectives and oversee the IS enterprise;
- A senior-level executive body that would provide strategic and policy direction, and whose members would be authorized to negotiate on behalf of and effect change within their respective department or agency with respect to IS matters;
- Subordinate coordinating bodies or subcommittee structure;
- Strong technical and policy engagement; consistent participation tracked and reported;
- Appropriate procedures and processes that effectively support the understood nature of the governance requirement;
- Governance entity to have its own self-sustaining technical capability:

---

<sup>16</sup> The ISST recommended that the IS governance entity be responsible for arbitrating differences among IS partner agencies. The concept of arbitration implies that issues would be decided by a neutral decision maker rather than by the parties themselves. The Task Force determined that the more appropriate difference-resolving construct for IS agencies would be for the IS partners to resolve their differences themselves with the help of a mediator, who would facilitate the conversation. There might also be situations in which arbitration by a neutral party might be helpful. The Task Force recommends a flexible approach that in general provides for mediation of agency differences, but also allows the agencies to elect arbitration on a voluntary basis when desired.

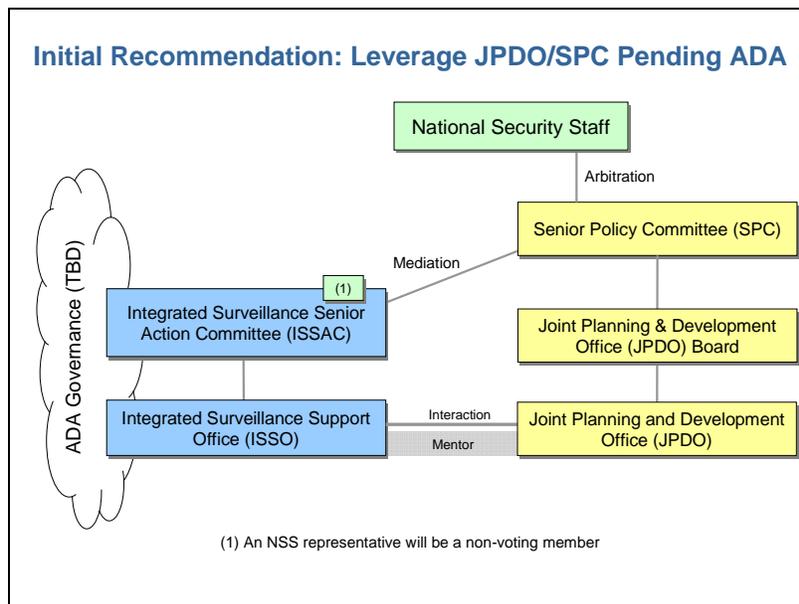
- Fully funded and staffed to accomplish the work assigned;
- Each agency provides people to these jobs and ties it into their performance plan, and/or the partners provide the money to hire a contractor to do the work;
- Knowledgeable about department/agency requirements and plans but able to function with considerations beyond their own departments' agenda;
- Acts as an honest broker whose mission is to build trusting relationships between partners in furtherance of a national integrated IS capability;
- Tracks actions for accountability.

### 2.3.2 Recommended IS Governance Entity

The Task Force acknowledges that establishment of IS Governance is proceeding as an independent activity in parallel with the broader interagency activity to develop governance for Air Domain Awareness (ADA). It is understood that in the future when ADA is better understood, the IS governance organization will either expand to incorporate ADA governance or the IS Governance organization will be incorporated as appropriate into the ADA structure.

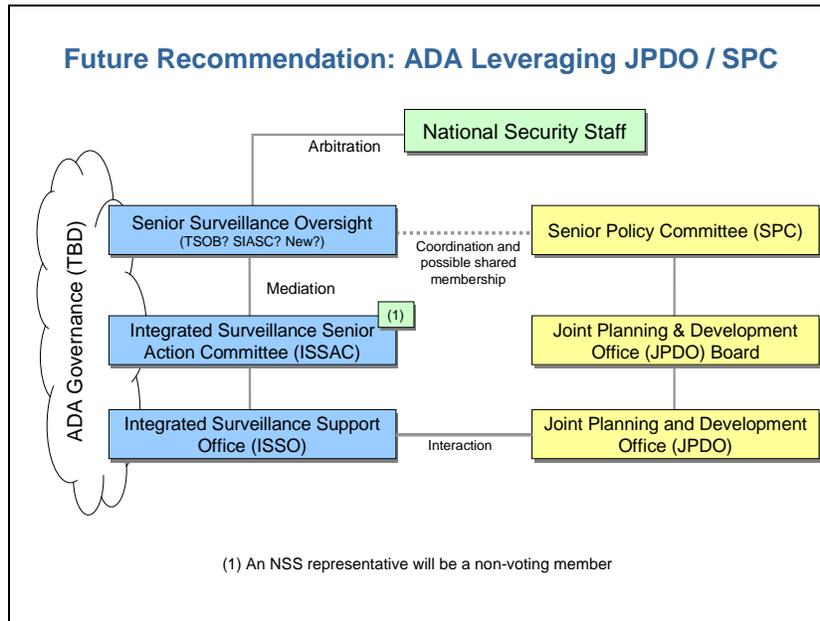
To be complementary to ongoing ADA deliberations, and in keeping with key principles stated above, the Task Force recommends that the organization depicted in Figure 1 below be established to manage IS services while governance of Air Domain Awareness (ADA) is being developed.

**Figure 1**



Organizational relationships might evolve as depicted in Figure 2 to be complementary to ADA governance when the ADA governance structure is established.

**Figure 2**



*Senior Surveillance Oversight (SSO).* The Task Force recommends that there be a Cabinet-level oversight function that sets overall goals and objectives for the national IS enterprise. The SSO would operate in a way consistent with the ADA governance structure once that structure is established. Until ADA governance is in place however, the Task Force recommends that the existing NextGen Senior Policy Committee perform the SSO role. In the ultimate ADA-conforming IS governance structure, the SSO role might be performed by a DHS-led interagency council such as the Transportation Security Oversight Board (TSOB)<sup>17</sup> or the yet-to-be-formed Standing Interagency Aviation Security Committee (SIASC).<sup>18</sup> The SSO would receive annual reports on progress, and mediate differences among departments and agencies that cannot be resolved at lower levels of the IS organization. The Task Force observed that one of the most commonly cited barriers to success in interagency endeavors is the tension executives experience when participating in joint activities that require them to subordinate their own agency goals and objectives to achieving collective and/or national benefits. NTIA/IRAC overcomes this issue by

<sup>17</sup>The 2001 Aviation and Transportation Security Act, 49 USC Section 115, established the TSOB. It is chaired by the Secretary of DHS and includes in its membership DoD, DHS, DOT, the Attorney General, Treasury, the CIA, and the NSC. Although the TSOB has been dormant since 2004, when active its main focus was aviation.

<sup>18</sup> The NSAS recommended establishment of the SIASC to support integration of surveillance and intelligence across the interagency space, and incorporate the primary Federal stakeholders. The SIASC would include the Departments of Homeland Security Defense, Transportation, State, Justice, Commerce, Energy, and ODNI. The SIASC has yet to be established.

NTIA having the final decision making authority among departments/agencies when it comes to spectrum allocations, which it exercises in the national interest. Since there is no single point of authority within the Federal Government for IS policy decisions, the Task Force borrowed from the PM-ISE exemplar and recommends a pathway upward from SSO through the NSS for arbitration of intractable differences among agencies when a national perspective is needed.

*The Integrated Surveillance Senior Action Committee (ISSAC).* The ISSAC would formulate policies for application to IS services. It would be chaired by DHS<sup>19</sup>, and composed of senior officials who would be knowledgeable about IS technical issues or have programmatic or budgetary influence over IS assets in their agencies. ISSAC members should be high enough in stature within their agency to negotiate on behalf of and effect change within their respective organizations, and to assure follow-through on collaboratively derived commitments. This recommendation is based on lessons learned through the exemplar analysis. It was observed that in both the PNT and NTIA/IRAC examples, achieving collaborative decisions on important issues and assuring follow through were often compromised because decision-making bodies were populated with subject matter experts (usually at the GS-15 level) rather than by more senior executives who have authority over budgets and resources. In the NTIA/IRAC example this deficiency is compensated for by the ability of NTIA to mediate issues among agencies from

---

<sup>19</sup> The Task Force recommends that DHS chair the ISSAC and eventually host the ISSO because this arrangement will be consistent with missions and responsibilities already assigned to DHS by Executive directives:

**Department of Homeland Security Authority from NSPD-47/HSPD-16.** The Secretary of Homeland Security is responsible for closely coordinating United States Government activities encompassing the national aviation security programs including identifying conflicting procedures, identifying vulnerabilities and consequences, and coordinating corresponding interagency solutions. In support of these responsibilities, the Secretary of Homeland Security:

- will conduct regular reviews of national aviation security programs to identify conflicting procedures, identify changes to threats, vulnerabilities, and resulting consequences, and coordinate corresponding interagency mitigation measures;
- will undertake additional initiatives, as appropriate, to maximize aviation security for the United States and its interests;
- is responsible for operational coordination with other United States Government departments and agencies, as well as with foreign governments, in the prevention of and response to aviation security incidents;
- is responsible for advancing common security interests in the Air Domain; and
- is responsible for effecting information sharing related to aviation security in support of an improved global aviation security network.

Source: NSAS

the position of regulator with the power to withdraw spectrum, but this situation is not ideal. The Task Force seeks to improve decision making in the IS organization by populating the ISSAC with members at a slightly higher level in their organization, but not at too high a level for that individual to have familiarity and knowledge of the technical and programmatic matters. Setting participation in the ISSAC at a senior management level also has the advantage that these individuals are more available—and more conversant with the issues—and therefore more likely to engage personally in the ISSAC than would be a Cabinet officer or deputy. The Task Force suggests that the NSS select an individual to be a non-voting member of the ISSAC to increase awareness by the NSS about IS activities. The Task Force recommends that attendance at ISSAC meetings be tracked and reported annually to the ISSAC and SSO function--a mechanism which in the IRAC case has boosted participation.

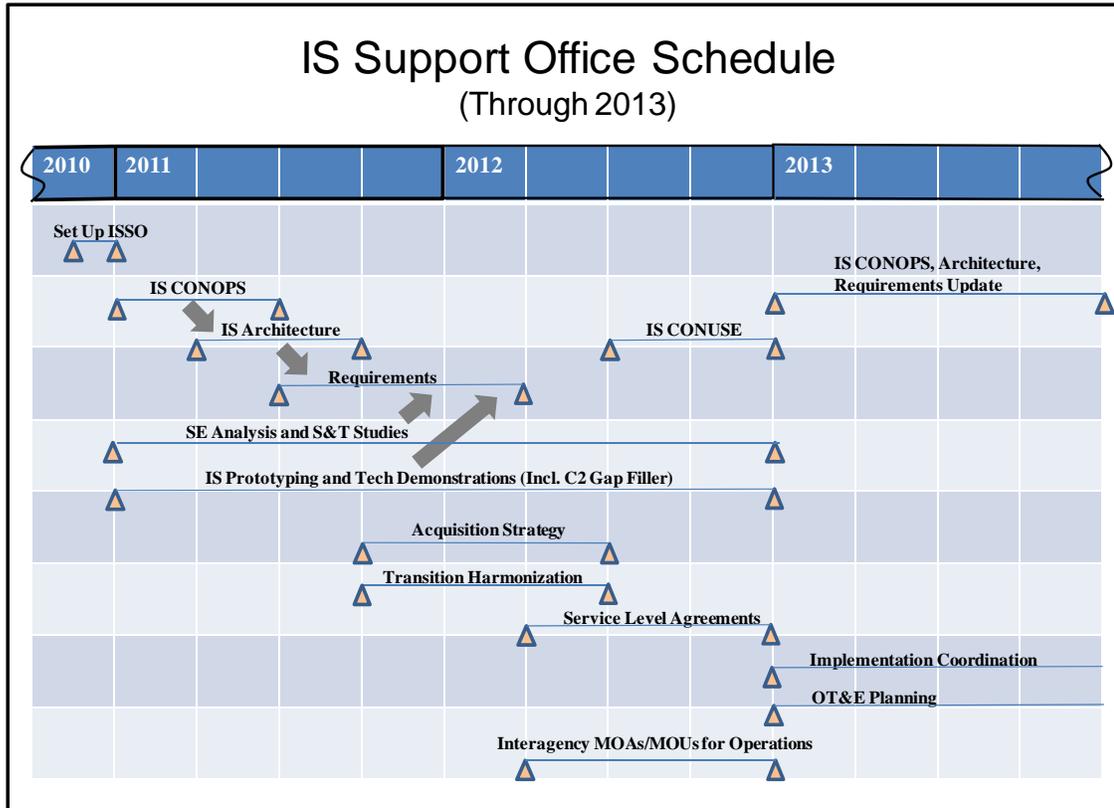
*ISSAC Subcommittees and Ad Hoc Working Groups.* Key to the success of all the interagency exemplars was well-staffed, effectively-managed technical work by subordinate bodies. The recommended IS organization charter states that the ISSAC may establish or eliminate subcommittees or other permanent or temporary groups as necessary or desired to perform work related to surveillance services, and that it shall at a minimum start with the following Standing Sub-Committees: (1) ConOps/Architecture, (2) Services Planning and Implementation, (3) Science and Technology, and (4) Interagency Services Operations. A common challenge among exemplars was how to leverage the output of committee members whose expertise was fairly specialized, and whose time commitment to the collective endeavor is limited. To address the resource issue the Task Force is first recommending that, to the greatest extent possible, the IS organization take advantage of the work already underway in other interagency organizations. To assure the cooperation of those groups, this report names relevant activities and encourages those bodies to assist the IS effort. Second, it was observed from all the exemplars that subgroups can be very productive when their work is organized, informed, and led by a well-staffed, dedicated technical support organization. The Task Force recommends similar resource—the ISSO--for the IS organization.

*Integrated Surveillance Support Office (ISSO).* The exemplar analysis clearly demonstrated that a well-resourced, dedicated technical support capability is essential to effectiveness of interagency collaboration. Although the executive model of governance is deemed not suitable for the IS environment, those exemplars who operated through the strong technical and managerial leadership of a program office (e.g., the Air Force as system provider in PNT, and ONC-HIT for NHIN) were most effective in fielding services and capabilities. To bring the same kind of effectiveness to the IS organization, the Task Force recommends the establishment of a well-resourced IS technical support office, the ISSO. Both the NTIA/IRAC and ONC-HIT exemplars demonstrate that to the extent the technical support office can be an “honest broker” among departments and agencies it will have better success mediating differences. For both NTIA/IRAC and ONC-HIT this characteristic is achieved by the technical support office being a

disinterested service provider/regulator, rather than a stakeholder in the outcome or products of the enterprise. To duplicate this “honest broker” characteristic in the IS organization, the Task Force is recommending that the ISSO Director, although technically a DHS employee, be selected and supervised by the ISSAC who would rate the Director’s performance on, among other factors, his or her ability to fairly mediate among IS partners. The Director’s office would have dedicated technical staff funded and/or staffed by the agencies who would be supervised and performance-rated by the ISSO Director. Not including the ISSO Director who will be a DHS employee, the ISSO will be funded by the IS partners as follows: 2/7 each by DoD, DHS and DOT, and 1/7 by DOC. In addition, the ODNI will provide support to the ISSO through the Air Domain Intelligence Integration (ADII) Element. The Mission of the ADII Element will be to “Optimize information sharing within the Global Air Domain Community of Interest by identifying barriers and defining solutions that provide a community-wide integrated information sharing capability to maximize Air Domain Awareness.” Full operational capability of the ADII Element is currently planned for FY 2012. To assure ISSO’s awareness of department/agency requirements IS departments and agencies also will have the opportunity to detail their own experts (government or contractor) in equal numbers to the ISSO. The ISSO will provide technical and administrative support to the ISSAC; and will chair, and provide technical and administrative support to the ISSAC sub-committees and sub-groups. The ISSO would develop staff positions and recommendations that would go forward to the ISSAC for formal consideration. The ISSO will provide an independent staff view of issues to support mediation services to the ISSAC and its sub-committees. The ISSO also would help IS agencies coordinate their efforts to keep Congressional committees aware and informed about interagency IS collaboration, including synchronization of program funding.

The fundamental work of the ISSO is to fulfill the integrated surveillance requirements set forth in the Integrated Surveillance Work Plan. The ISSO’s work comprises four task areas: system engineering, implementation coordination, operations monitoring, and administrative efforts. The following paragraphs summarize the products of each task area and indicate the ISSO’s effort for the first two years to lead the necessary product development tasks. Based on this report’s analysis, 11 ½ full time equivalents (FTE) of effort are required by the ISSO to lead, document, coordinate and provide the core technical staff for each of the first two years. It is expected that the agencies will provide agency representatives to augment the ISSO staff and contribute to the development of each product, serving as subject matter experts and liaisons to their agency’s leadership. Figure 3 provides a schedule for ISSO product development and indicates some of the dependencies. In the following sections product descriptions are provided in each task area with the total effort, in Full Time Equivalents (FTE), indicated for each product developed for the first two years of the ISSO. During product development the ISSO, in coordination with the agency representatives, will determine the need for classified portions for each IS product.

Figure 3



**System Engineering (CONOPS, CONUSE, Architecture, Requirements, and Related Tasks)**

System engineering starts with the IS ConOps and progresses to architecture, requirements, allocation to agencies, transition planning, risk management, and identification of areas for improvement based upon operational experience. Detailed requirements work, system acquisition, and implementation would be addressed by each agency and coordinated by the ISSO. The major system engineering products are:

- Concept of Operations (2FTE) – Communicates overall quantitative and qualitative system of system characteristics to the user, acquirer, developer, and other organizational elements (e.g., training, facilities, staffing, and maintenance). Represents the further development of the “high level” IS ConOps developed through the JPDO with the agencies. This is a primary driver for the IS architecture effort.

- Concept of Use / Concept of Employment (2 FTE) – Describes the manner that the system-of-systems will be used and suggests changes to tactics, techniques, procedures, regulations, laws, or doctrine, and their civil equivalents.
- Integrated Surveillance Architecture (2.5 FTE) – Describes baseline and needed capabilities (including operational improvements). Represents the further development of the IS architecture developed through the JPDO and includes capability, operational, system, and technical perspectives in addition to the relationship with the external environment. The architecture will depict the IS system-of-systems and show the federation of the individual agency surveillance capabilities. This is a primary driver for the IS requirements effort.
- System Engineering Analyses and Science & Technology Studies (2 FTE) – This includes the conduct of analyses and studies to support development of the ConOps, Concept of Use, architecture, and requirements documents. The ISSO, in consultation with the agencies, will select the appropriate topics for analysis and study.
- IS Prototyping and Technology Demonstrations (2 FTE) – This includes planning and coordination of prototyping activities for IS and will leverage existing efforts, such as the C2 Gap Filler Joint Concept Technology Demonstration. The lessons learned will be used to mature the ConOps, architecture, requirements, and reduce risks.
- Requirements (1.5 FTE) – This is the master requirements document that shows the top level requirements that are allocated to agencies with traceability to IS ConOps, Concept of Use, and architecture. This is a primary driver for the agency detailed requirement definition and implementation efforts.

## **Implementation Coordination**

Implementation coordination includes acquisition strategy, transition harmonization, and operational test and evaluation. The total effort, in full time equivalents (FTE) is indicated for each product. Major implementation coordination activities and products are:

- Acquisition Strategy (1 FTE) – Agencies will participate in collaborative investment strategy development to support reaching agreement on IS investments and their priorities. An IS business case will be developed. The acquisition strategy includes long-term investments for cooperative research and development. An integrated funding strategy is coordinated with OMB.
- Transition Harmonization (1.25 FTE) – System implementation, including transition roadmap (i.e. integrated master schedule), to achieve operational IS capability. This references surveillance portions of agency transition plans. The plan includes key decision points and a critical path. It is used to manage synchronization across the agencies and programs, and to assess ripple effects when issues arise. Synchronization includes interaction with complementary activities such as those identified in section 2.3.3 and 2.3.5 of this report.
- Service Level Agreements (SLAs) (1 FTE) – SLAs are developed between the agencies to identify network requirements and needs for service integration, provisioning and maintenance across the IS community. These will be used to manage and assess operations, including qualities of service, between the agencies. The SLAs will be documented in the interagency MOUs/MOAs.
- Implementation Coordination and Monitoring – IS “program management reviews” are conducted periodically (e.g. semi-annually). A risk management effort is developed and implemented.
- Operational Test and Evaluation – This includes planning and conducting operational test and evaluation for the interagency IS capability and system. This verifies that the implementation by the agencies satisfies the IS ConOps, architecture, requirements, and SLAs.

## **Operations Monitoring**

Operations monitoring is performed to develop status reports for the agencies and to identify areas for enhancement or to address deficiencies.

- Generate interagency MOAs/MOUs (0.75 FTE) – These are agreements as to the manner that the agencies would work together in operating the IS capability.
- Monitor Operations – This includes development of periodic operational status reports used to identify enhancements, improvements, problems needing remediation, etc.

### **Management and Administration**

Management and administration includes setting up the ISSO, assigning leadership and obtaining support staff, identifying the needs for resources, developing IS program status reports, and coordinating policy guidance (3 ½ FTE for each of the two years).

*Relationship with Air Domain Awareness Governance.* At the time of this writing, the governance structure for national Air Domain Awareness had yet to be established. The Task Force acknowledges that establishment of IS Governance is proceeding as an independent activity in parallel with the broader interagency activity to develop governance for Air Domain Awareness (ADA). It is understood that in the future when ADA is better understood, the IS governance organization will either expand to incorporate ADA governance or the IS Governance organization will be incorporated as appropriate into the ADA structure. Until the ADA structure is established (expected to take 18 to 24 months) and a permanent location for the IS entity is designated, the Task Force recommends that the ISSO leverage existing resources by setting up residence in the JPDO. During this interim period JPDO, which has appropriate technical expertise and facilities suitable for housing the IS activity, would support the initial start up of ISSO including the development of a work plan and staffing recommendations, and provide core support to the ISSAC subcommittees and ad hoc working groups. During this period the SPC would perform the functions of the SSO.

### **2.3.3 External Factors Recommended for Success**

During the course of exemplar analysis, it became clear to the Task Force that a well-designed organization and adequate resources were not sufficient for success of interagency collaboration. Those organizations which were most effective also benefited from some external advantages. The Task Force recommends that the following additional measures would improve the prospects for successful interagency management of IS services.

*Top-down Executive Engagement.* The Task Force was concerned about how to encourage top-level engagement of senior government executives in IS matters, and how to assure survival of

gains in interagency management of IS services during administration changes or other disruptions. The Task Force noted that all of the exemplars were established through legislation, by Presidential directive or executive order, or in some cases by both. The Task Force considers it essential for success that the IS governance organization be established and empowered through a Presidential Executive Order or Directive, as part of a more comprehensive directive establishing ADA governance or, if necessary, dedicated solely to IS governance. Moreover, as the PM-ISE exemplar demonstrates, executive-level authorization will not be sufficient. Regardless what form the top-down direction takes it will be essential for success that Cabinet-level support for the IS initiative be visible and persistent. To achieve this level of top-down engagement the Task Force recommends that, in addition to an unambiguous Presidential mandate, a reporting structure for the IS entity be established that proceeds upward to a Cabinet-level oversight body (SSO) and then use the NSS process when consensus among IS departments and agencies cannot be achieved.

*OMB Engagement.* Exemplar analysis revealed that the most significant advantage of the executive governance model was the ability to assure reliable funding and consistent program management of interagency services and capabilities (e.g., ONC-HIT, and AF management of GPS programs.) On the other hand, in the case of the PNT organization, the lack of an effective mechanism for assuring alignment of individual agency investments in augmentations and GPS civil applications was cited as a major obstacle to effective interagency management of joint civil GPS requirements. As stated earlier, joint program management of IS services is not considered practical or desirable. But it is clear that bringing some measure of budget discipline to the IS enterprise would facilitate synchronization of department/agency activities. IS will require an integrated interagency investment strategy, and it will be important that the OMB, and Congressional committees and their budgeting officials understand that individual agency systems and capabilities build upon each other to deliver integrated services. The Task Force therefore recommends that OMB have regular visibility into IS organization activities. This could be achieved by inviting, and actively recruiting, a senior-level level OMB official to be an observer of SSO and ISSAC deliberations, by requesting that all the partner agency OMB examiners be made responsible for coordinating IS issues within OMB, and by encouraging the ISSO Director to establish a working relationship with OMB officials at the appropriate level.

### **2.3.4 Transition Recommendation**

The Task Force recommends that, pending establishment of ADA governance, the SPC take the following steps to implement an interim IS governance organization as early as September 2010<sup>20</sup>, so that work can proceed immediately on interagency planning and implementation of IS services:

---

<sup>20</sup> See Figure 3. This aggressive schedule is intended to produce engineering results that will be incorporated into 2012 budget formulation activities.

- Stand up of the ISSAC and ISSO structure within the JPDO under SPC policy guidance and oversight
- Direct the IS organization to begin needed system engineering, implementation coordination, operations monitoring, and administrative efforts,
- Inform the appropriate National Security Staff of these interim steps to advance the national integrated surveillance capability; and
- Direct IS departments to develop and sign an interagency IS governance MOA.

The SPC also should seek issuance of an Executive directive within 18-24 months establishing ADA governance that incorporates the IS activity, and align ongoing IS activity within the ADA organization.

### **2.3.5 Relationships to Complementary Activities**

There are several interagency bodies with which the eventual IS Governance structure should interact in order to maximize National capabilities and minimize unnecessary resource demands. The lash-up of these interagency mechanisms with the proposed IS Governance mechanism should address reconciling any overlaps and coordinating policy, requirements, funding, plans or operations of the nation's aviation transportation system surveillance assets and leverage the work of these bodies to further the IS enterprise. The following entities should be engaged on a regular basis:

#### **2.3.5.1 Director of National Intelligence (DNI):**

Global Maritime & Aviation Intelligence Integration (GMAII)...for interagency perspective relative to surveillance, architecture, intelligence integration, and--where appropriate--maritime complements.

The GMAII staff endeavors to ensure effective Community of Interest-wide access to air/maritime surveillance and intelligence information, analysis, and data critical to enable policy and operational decision-makers. Their efforts are intended to help provide guidance and oversight to interagency intelligence enterprise to improve availability and integration of air/maritime surveillance and intelligence information. As such, the GMAII director submits an annual report to DNI, DoD, DHS, DOJ, DOS, and DOT regarding the status of the intelligence enterprise, and is charged to recommend changes to authorities, responsibilities, programs, and operations of enterprise members.

Program Manager – Information Sharing Environment (PM-ISE)...for interagency perspective and national-level information sharing coordination for cross domains.

PM-ISE oversees the fulfillment of the Intelligence Reform & Terrorism Prevention Act of 2004, Executive Orders, and Presidential Guidelines on planning, managing, and overseeing government-wide terrorism-related information sharing. The principal nexus of

this partnership lies in network-centric operations, security management, and OMB relationships which may significantly enhance surveillance services capabilities. PM-ISE staff is currently leading or supporting seven tasks in close relationship with the NSS' Information Sharing & Access IPC.

### **2.3.5.2 Department of Homeland Security (DHS):**

Domestic Nuclear Detection Office (DNDO)...for surveillance architecture, detection capabilities, and integrated operational environment.

The Domestic Nuclear Detection Office (DNDO) is a jointly staffed office established April 15, 2005 to improve the Nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the Nation, and to further enhance this capability over time. DNDO has an evolving and growing interest in aviation surveillance capabilities and elements of DNDO are charged with key mission areas, some of which are applicable to integrated surveillance, such as:

- identifying gaps and vulnerabilities in the existing global nuclear detection architecture;
- carrying out the engineering development, procurement and deployment of current and next-generation nuclear detection systems (includes surveillance);
- developing the information sharing and analytical tools necessary to create a fully integrated operating environment, among others.

### Transportation Security Oversight Board (TSOB)

The 2001 Aviation and Transportation Security Act, 49 USC Section 115, established the TSOB. It is chaired by the Secretary of DHS and includes in its membership DoD, DHS, DOT. Although the TSOB has been dormant since 2004, when active its main focus has been aviation. Should TSOB become active again, expansion of membership would need to include DOC and DNI for purposes of integrated surveillance. The placement of any Integrated Surveillance Governance or future growth of such governance into Air Domain Awareness (ADA) governance must account for TSOB as a legislated body and the corresponding relationship.

### **2.3.5.3 Department of Commerce (DOC):**

Office of the Federal Coordinator for Meteorology...for surveillance of meteorological phenomena and potential for multi-function surveillance capability.

The Department of Commerce formed the OFCM in 1964 in response to Public Law 87-843 and was established because Congress and the Executive Office of the President recognized the importance of full coordination of federal meteorological activities. Their mission is to ensure the effective use of federal meteorological resources by leading the systematic coordination of operational weather requirements and services, and supporting research, among the federal agencies. Fifteen federal departments and agencies are currently engaged in meteorological

activities and participate in the OFCM's coordination and cooperation infrastructure. The OFCM carries out its tasks through an interagency staff working with representatives from the federal agencies who serve on program councils, committees, working groups, and joint action groups. This infrastructure supports all of the federal agencies that are engaged in meteorological activities or have a need for meteorological services. In addition to providing this coordinating infrastructure, the OFCM prepares operations plans, conducts studies, and responds to special inquiries and investigations. The OFCM recently restructured the interagency coordinating process to better match the federal agencies' perspectives, focus areas, and priorities for the 21st Century and, at the same time, reduced the number of groups needed to support the infrastructure.

#### **2.3.5.4 Department of Defense (DoD):**

Capabilities Development Working Group (CDWG)...for interdepartmental research, development, experimentation, test, and acquisition opportunities.

The DoD Homeland Defense and Civil Support Strategy (June 2005) called for “close cooperation with the DHS” and for “nurturing new collaborative research, development, experimentation, test and acquisition opportunities with DHS, while avoiding duplication of efforts in these areas.” Hence, the chartered CDWG has as objectives: provide a senior level forum for DoD and DHS to explore capability development topics of mutual interest; ensure best use of resources and avoid duplication of effort; promote further cooperation as appropriate; and support/inform policy, planning, and decision-making activities. The DoD-DHS CDWG is led jointly by the DoD Under Secretary for Acquisitions, Technology, and Logistics (AT&L), the DHS Under Secretary for Science & Technology (S&T), and the DHS Under Secretary for Management (M). Other invited members include the Assistant Secretary of Defense (ASD) for Homeland Defense and America Security Affairs, the Director of the Joint Staff, the Commander of NORTHCOM/NORAD and the Chief of the National Guard Bureau (NGB). Additional Federal Government organizations may be considered for invitation as appropriate. This body routinely addresses Air Domain and Integrated Surveillance concerns and capabilities.

Long Range Radar Joint Planning Office (LRR JPO)...for non-cooperative surveillance management, acquisition, and test-bed initiatives.

Long Range Radar Joint Program Office (LRR JPO) was created in 2005 to establish relationships between the DoD/DHS Offices of Primary Responsibility for oversight and management of the Operations and Maintenance of the LRR and associated air navigation, surveillance and communications systems as well as the Service Life Extension Program of the legacy radars. The mission of the LRR JPO, located at Langley AFB, is to Support Air Defense (AD) and DHS missions. Primary focus is on the AD/DHS radar networks with key interests in Joint use long-range radars (ARSR-4, ARSR-3, ARSR-1/2 and FPS-20 series), FAA and DoD short-range radars, and Tethered Aerostat Radar System (TARS). The LRR JPO has worked with the DoD, DHS, and DOT/FAA on an Obstruction Analysis Assessment process that dealt

with wind turbines, large diameter structures (i.e., buildings, tanks, etc.), and small diameter structures (i.e., towers, antennas, etc.)

Maritime Domain Awareness (MDA)...for the overlap areas of aviation surveillance, surveillance initiatives in general, and for the future integrated domain awareness.

The national and joint efforts, as outlined in the National Plan to Achieve Maritime Domain Awareness (NPAMDA), have developed an assortment of potential areas to leverage for aviation governance. Such areas are their stakeholders' board, a National Maritime Domain Awareness (MDA) Interagency Investment Strategy (IAIS), and the National Concept of Operations for MDA, among others. The efforts provide a framework for the MDA Stakeholder Board to coordinate existing and future MDA initiatives across the Federal Government and prevent unnecessary duplication.

Joint Integrated Air & Missile Defense Organization (JIAMDO)...for interagency and DoD specific surveillance studies, architecture, and initiatives synchronization.

JIAMDO is chartered to plan, coordinate, and oversee Joint Air and Missile Defense (AMD) requirements, joint operational concepts, and operational architectures, and supports the Chairman, Joint Chiefs of Staff in meeting Title 10 responsibilities as they relate to air and missile defense issues. JIAMDO serves as the operational community's proponent for characteristics, requirements, and capabilities in air and missile defense, and is the joint air and missile defense resource proponent within the DoD's resource allocation structures. Among other responsibilities applicable to surveillance, JIAMDO provides direct support to NORAD and the US Northern Command (USNORTHCOM) for homeland air surveillance issues and to the US Joint Forces Command (USJFCOM) for capabilities development and validation in support of its Unified Command Plan (UCP) assigned missions. JIAMDO is the proponent for the Homeland Air & Cruise Missile Defense (HACMD) of North America analysis which has received DoD's Joint Requirements Oversight Council endorsement. JIAMDO is an active participant among interagency integrated surveillance forum and development activities.

### **2.3.5.5 Department of Transportation (DOT):**

Joint Planning & Development Office (JPDO)...for initial nesting and nurture of ISSO, and bridging collaborative interagency surveillance to NextGen.

Public Law 108-176 established the JPDO which is comprised of the relevant Departments for integrated surveillance. DoD, DHS, DOT, FAA, DOC, and DNI have enormous equities for ensuring Integrated Surveillance improves during the transformation development of NextGen. Integrated Surveillance common services are foundational for NextGen and considered a pillar of the larger Air Domain. It is crucial for any IS governance mechanism to account for NextGen development and inform every aspect of NextGen planning.

### **2.3.5.6 Executive Office of the President**

National Security Staff (NSS)...for interagency success, congruence, and if necessary, arbitration.

The IS Governance mechanism must appropriately interact and intersect with the NSS. The Cabinet-level “Seniors” should connect with the appropriate level, PC and/or DC and through the Interagency Policy Committees, such as Transborder Security and/or Information Sharing & Access IPCs. The construct of interaction and intersection may involve issues needing arbitration at the Senior level, while coordination and awareness occurs at the IPC level.

Office of Management & Budget (OMB)...for insight of integrated surveillance efforts to align budget and management.

The Task Force recommends that OMB have regular visibility into IS organization activities as described in 2.3.3.

**2.3.5.7 Joint (Interagency) Operations Centers**...for operational impact, such as operations insight into policy and plans formulation and subsequent metrics to feedback the results for verification of the expected outcome.

IS Governance should rely on operationally focused entities for expertise in areas such as concept of operations, architecture descriptions, requirements, and plans. Additionally, these operational entities should provide feedback on policy and technology application success or shortcomings. Examples are:

- Customs & Border Protection Air & Marine Operations Center (AMOC)
- NORAD-USNORTHCOM operations centers Joint Interagency Task Force-South (JIATF-South) operations center
- Freedom Center (formerly the Transportation Security Operations Center (TSOC)).

**2.3.5.8 Joint/Interagency Technology Demonstrations**...for evolving research and development and verification of potential concepts.

IS Governance should rely on current and future IS-related experiments and demonstrations. These efforts can help resolve identified policy and technology issues. Any leave-behind joint capability or governance entity must conform to these IS Governance-developed plans and policies and support convergence and on-going maintenance of the IS CONOPS and EA. Examples are as follows:

- Joint Capabilities Technology Demonstrations such as Command & Control (C2) Gap Filler

- Program offices such as the Long Range Radar (LRR) Joint Program Office (JPO) test-site at FAA's Mike Monroney Center
- Multi-Function Phased Array Radar (MPAR) Development and Test Site coordinated by OFCM with FAA, DoD, DHS, and NOAA participating
- Maritime Domain Demonstrations, led by DoD (USN) and/or DHS (USCG) that have aviation application.

## DOCUMENT REVISION HISTORY

VERSION	DATE	DESCRIPTION
---	December 16, 2009	Integrated Surveillance (IS) Senior Advisors Confirmation of Governance Key Characteristics
Draft Version 0.1	January 20, 2010	Draft written by IS Core Team
Draft Version 0.1	January 25, 2010	Draft transmitted to IS Agency Leads
Draft Version 0.1	January 29, 2010	Draft revised based on comments received
Draft Version 0.2	February 5, 2010	Draft transmitted to IS Agency Leads
Draft Version 0.2	February 17, 2010	Draft revised based on comments received
Draft Version 0.3	February 19, 2010	Draft transmitted to IS Senior Advisors
Draft Version 0.3	February 19, 2010	Draft transmitted to JPDO Division Directors
Draft Version 0.3	March 10, 2010	Draft revised based on comments received
Draft Version 0.4	April 14, 2010	Adjusted Draft transmitted to the IS Senior Advisors
Draft Version 0.5	April 29, 2010	Adjusted Draft transmitted to the JPDO Board for Formal Review
Draft Version 0.5	May 24, 2010	Critical comments received from JPDO Board
Draft Version 0.5	June 1, 2010	IS Senior Advisors Meeting with Agency Leads
Draft Version 0.6	June 8, 2010	Adjusted Draft transmitted to the JPDO Board for Formal Review.
Draft Version 0.6	June 22, 2010	Critical comments received from JPDO Board

# APPENDIX A

## *Exemplars Examination and Analysis*

Following is a summary of information the Task Force gathered about each of the four exemplars.

PNT ExCom/National Coordination Office. The National Space-Based Position, Navigation, and Timing (PNT) structure, established by Presidential directive in 2004, provides for joint (DoD services/agencies participation in the management and acquisition of the Global Positioning Satellite (GPS) system acquisition program. The Secretary of the Air Force, as Executive Agency for Space, has the responsibility for developing, acquiring and maintaining the major components of GPS. The National Space-Based PNT Executive Committee (PNT ExCom), co-chaired by the Deputy Secretaries of Defense and Transportation, is the collaborative interagency body through which interagency issues related to GPS are considered. Other members of the PNT ExCom (Deputy Secretary-level) are the Departments of State, Interior, Agriculture, Commerce and Homeland Security, the DoD Joint Chiefs of Staff, and NASA. The PNT ExCom has an Advisory Board sponsored by NASA which includes experts from the private sector.

In the PNT ExCom, the Secretary of Transportation represents the interests of civil departments/agencies in connection with GPS needs and acquisition issues, including arranging agency funding for new civil unique requirements. DOT fulfills this responsibility through a GPS Wing Program Manager for Civil Applications. This office does not have a significant dedicated technical staff.

Work of the interagency ExCom is performed through a National Coordination Office (NCO), hosted by the Department of Commerce, and staffed with expertise assigned by the member agencies (GS 15 level). The NCO has a GPS International Working Group chaired by DOS, an Engineering Forum co-chaired by DoD and DOT, and other ad hoc working groups. The PNT ExCom/NCO uses the following tools of coordination. The first is a Five-Year National Space-Based PNT Plan, which summarizes the individual agencies' PNT plans. The second is the Interference and Protection Plan, whereby DHS coordinates Coast Guard's capabilities to detect and mitigate interference to GPS and augmentation systems. Third is a National PNT Architecture, which provides a framework/investment strategy to help guide future PNT system-of-systems investment for the 2025 timeframe. Fourth is the International Strategy for Cooperation and Consultation, to achieve compatibility and Interoperability with other foreign systems. Fifth, the PNT ExCom/NCO makes an annual report to the President.

The PNT ExCom has a process for coordinating interagency GPS requirements, the Interagency Forum for Operational Requirements (IFOR), with the object of getting civil requirements integrated into GPS planning. In general, PNT expenditures consist of DOD funding for GPS infrastructure/services and simultaneous expenditures of civil agencies for augmentations and individual mission needs, synchronized with DoD plans. There is no joint decision making on combined National requirements at this point, although the IFOR is working toward the goal of a joint civil requirements document. Historically civil agencies have found it advantageous to “piggy back” on DoD systems, rather than stating requirements and providing the corresponding funding.

There was general agreement on the PNT model's strong organizational structure and ability to mediate – but not to arbitrate – policy issues through discussion among senior representation. A key take away from this exemplar is the need for an interagency entity to have a mechanism for arbitration of policy issues if the status quo is to be changed.

With respect to requirements generation, there was general agreement that the model in practice has been able to document civil/military requirements. Similarly, with respect to effectiveness of technology maturation, there was general agreement that PNT offers a good way to share information. However, without any real mechanism to unify and catalyze the involved agencies into concerted action, the tendency for each agency to “do what we were already doing” is largely prevalent. The Task Force believes that a more robust technical capability within the NCO would be necessary to achieve the synergies of truly integrated requirements and R&D.

The Task Force considered the PNT entity's ability to synchronize and arbitrate funding issues directly related to the ability to generate requirements. Although the Task Force recognized the PNT ExCom's value as a multi-agency forum, they noted that the organization does not control funding and does not have a mechanism to force concerted action and ensure an equitable division of funding obligations. Funding for the PNT NCO support activity is shared, but minimal. There was agreement that a robust independent technical ability to synchronize and adjust budgets is needed. With respect to the ability of the PNT structure to synchronize and arbitrate acquisitions, the Task Force noted that PNT has an established national strategy against which agency acquisitions could be aligned, as well as funding commitment from members and advice from the Advisory Board. Concerns remain however regarding the lack of a joint program authority, lack of a mechanism to arbitrate acquisition decisions across agencies, possible duplication of capabilities, and that the agency-defined roles may not properly reflect the use of the system.

With respect to synchronization and arbitration of PNT operations, this function is not within the PNT/NCO charter.

Concerning enforcement of joint decisions, there is no process within the PNT structure for accountability for individual agency commitments. The mechanism to enforce decisions seems to depend on the influence of senior leaders.

And regarding the ability of the PNT structure to mediate among diverse agency missions, Task Force members expressed concern over the differing objectives of PNT group members and the lack of a mechanism to ensure minority views are taken into account. There is evident difficulty in convincing agencies to subordinate individual missions to the overall national good.

NTIA/IRAC. The Interdepartment Radio Advisory Committee (IRAC), established pursuant to federal legislation and executive order, is the interagency body which provides information and policy input on federal agency requirements for radio spectrum. This input is to the National Telecommunications and Information Administration (NTIA), the decision making body that manages federal department/agency use of the Nation's radio spectrum. The FCC, which coordinates with NTIA, manages radio spectrum allocated for non-federal use including the private sector, and state and local government.

NTIA's role is regulatory rather than service provision. It is funded 20% directly by Congress for activity of the Office of Spectrum Management; the other 80% is funded by participating agencies, allocated according to a formula based on license fees for spectrum use and accounted for in individual agency budgets. The funding is transferred to NTIA through annual MOAs, which is seen as an exceedingly cumbersome process. NTIA does support some R&D, but this is primarily focused on leveraging work being conducted elsewhere on technologies to address frequency interferences.

NTIA chairs the IRAC, and full-time NTIA personnel chair the various IRAC subcommittees and other subordinate bodies. IRAC subcommittees and other groups are composed of subject matter experts from the various federal agencies (GS 15 level). The committees are collegial bodies that make decisions by consensus, and operate in accordance with extensive, regular rules of engagement embodied in the "Manual of Regulations and Procedures for Federal Radio Frequency Management" (Red Book). If a committee has an issue on which agreement cannot be reached, it can push the matter up to the IRAC. If the IRAC has an issue on which agreement cannot be reached, it can push the matter up to the Office of Spectrum Management for decision.

The NTIA/IRAC model appears to be very effective largely because, as a regulatory entity, NTIA is not an interested stakeholder in federal spectrum allocation decisions and therefore its staff can act as a neutral mediator among IRAC agencies. Also, NTIA has decision making authority over federal agency spectrum use and can withdraw spectrum and reallocate it among agencies if necessary. This enforcement capability contributes to its effectiveness in engaging senior agency management if necessary, and in mediating among agencies with diverse missions.

The IRAC Red Book states expectations for meeting attendance, and NTIA staff tracks and reports attendance of agency representatives in IRAC meetings to assure continuity of participation. This metric appears to be effective in increasing the level of participation in IRAC activities.

IRAC does not engage in requirements generation (this takes place on the individual agency level), collective technology maturation, or system acquisition. With respect to its ability to synchronize and arbitrate agency activities in policy development, there was overall agreement that the organization arbitrates fairly well. Federal law gives NTIA authority over federal users of the spectrum. NTIA serves to adjudicate problems if consensus is not reached in the IRAC. There is a dedicated Office of Policy Analysis and Development (which itself has divisions devoted to Domestic Spectrum Policy and IRAC Support, and International Spectrum Plans and Policy), and private sector involvement is also allowed via the Commerce Spectrum Management Advisory Committee (CSMAC). The Task Force had concerns, however, that much of the NTIA/IRAC's effectiveness—in terms of collegiality and joint decision making—stems from the personalities of the NTIA staff, and that this effectiveness may be at risk when membership changes.

Concerning IRAC's ability to synchronize and arbitrate members' operational issues, there was agreement that the governance structure allows NTIA to arbitrate among users. Working arrangements are made at the sub-committee levels and most decisions are based on technical and practical policy. However the Task Force is concerned that the exemplar does not have an internal enforcement structure, and the success is tied to the people rather than the structure.

Concerning synchronization and arbitration of funding issues, because of NTIA's regulatory rather than service provision mission, the analysis was limited to funding of NTIA/IRAC itself. The Task Force thought that the approach of 20 % appropriated directly by Congress and 80% coming from agencies is neither efficient nor easy. New MOAs are required annually. With respect to synchronizing and arbitrating operations issues, as with policy the Task Force agreed that the structure allows NTIA to arbitrate between users. Working arrangements have been made at the sub-committee levels and most decisions are based on technical and practical policy.

Concerning the ability of NTIA/IRAC to hold participants accountable, there was agreement that the model's structure ensures that NTIA has the ability to enforce decisions. Users must be licensed by NTIA, and the NTIA/IRAC structure allows issues to be raised to the Assistant Secretary level if necessary. As much as possible NTIA takes into consideration agency issues and limitations, and works with them toward solutions rather than exercising enforcement authority.

And with respect to the NTIA/IRAC's ability to reconcile diverse agency missions, there was general agreement that this area is one of NTIA/IRACs greatest strengths. As an impartial organization NTIA has the ability to arbitrate and has been able to use its technology research

arm to find mutually beneficial situations. Further, there is good multi-agency participation on IRAC subcommittees which assists in creating a consensus around issues. However, there is concern that NTIA/IRAC's effectiveness in this area is too linked to their people and the relationships they have created with their counterparts in the agencies. A change in personnel could be problematic, putting the level of knowledge and expertise in IRAC at risk.

Office of the National Coordinator for Health Information Technology (ONC/HIT). The Federal Health Architecture (FHA) is an E-Government initiative managed by the Office of National Coordinator for Health Information Technology (ONC-HIT) in the Department of Health and Human Services. The position of National Coordinator was created in 2004 through an Executive Order, and legislatively mandated in the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009.

Federal agencies determined there was a need to share patient health information among each other in order to increase the quality of medical care, increase patient safety, and decrease overall costs. This is achieved through a Nationwide Health Information Network (NHIN), a system of interconnected IT standards, technologies, and trust tools developed and made available to agencies by the ONC-HIT. Among these products is CONNECT, a federally-developed open source software solution that allows agency systems to exchange health information securely. More than 20 federal government agencies now participate in the FHA. The goal is for the NHIN to become a national network incorporating state and local entities and the private sector, including hospitals, doctors and other patient care providers.

ONC-HIT benefits from the recent emphasis and national attention being generated by President Obama's explicit policy in support of improved health care services IT.

The ONC-HIT performs its work through a program office in the Department of Health and Human Services. ONC/HIT receives its strategic guidance from the Managing Lead Partner Council (MLPC), composed of Chief Information Officer (CIO)-level executives of the federal agencies primarily funding FHA initiatives (DoD, Department of Veterans Affairs, and HHS). The Leadership Council (LC) is a larger group including all federal agencies whose missions include any health related activity. The LC provides program level input. The ONC-HIT staff interacts with work groups and task forces of the LC to develop information sharing requirements which are considered for implementation in quarterly ONC-HIT requirements reviews. ONC-HIT makes program decisions. Agencies stating the requirement for an IT product are expected to provide the funding for its production. ONC-HIT also is advised by two Federal Advisory Committees (FACAs), the Health IT Policy Committee and the Health IT Standards Committee, both established in 2009.

The ONC-HIT primarily exhibits the characteristics of the executive governance model, with ONC-HIT operating as a program office that gathers and develops agency requirements. ONC-

HIT then develops, tests, and delivers products and services as required and paid for by the requesting agency. This method of operations seeks to further national health care objectives by encouraging all health care service providers at all levels, public and private, to take advantage of IT improvements being implemented by the government. To the extent ONC-HIT operates in accordance with strategic and policy guidance of a Managing Lead Partner Council and Leadership Council, the total structure exhibits characteristics of a consortium. Going forward, ONC/HIT will be advised by two FACAs which are likely to push ONC-HIT more in a consortium direction.

PM-ISE. The Task Force examined the Program Manager-Information Sharing Environment (PM-ISE) governance structure through literature review and ongoing JPDO staff interaction. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended, called for the development of an ISE to provide and facilitate the "means for sharing terrorism information among all appropriate Federal, State, local and tribal entities, foreign partners, and the private sector through the use of policy guidance and technologies." The law also required the President to designate a Program Manager for the ISE, which in June 2005 he placed administratively under the Office of the Director of National Intelligence (DNI).<sup>21</sup> IRTPA also required the president to establish an Information Sharing Council (ISC), to advise the President and the Program Manager on the development of ISE policies, procedures, guidelines, and standards, and to ensure proper coordination among Federal departments and agencies participating in the ISE.

As described in the November 2006 ISE Implementation Plan, ISE activity was initially designed to proceed along two tracks. On a decision making level, the President would determine and enforce the policies and rules that govern the content and usage of the ISE. The Executive Office of the President would be informed by the Information Sharing Policy Coordination Committee (ISPCC), chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC). The ISPCC was made up of department representatives and was established to address major information sharing policy issues, including resolving issues raised by the PM-ISE, and to provide policy analysis and recommendations for decision by the Deputies or Principals of organizations represented on the HSC and NSC. The PM-ISE was made a member of the ISPCC, and was to participate in the HSC/NSC Deputies Committee on ISE. On April 10, 2007 functions<sup>22</sup> of the President under Section 1016(b) of IRTPA were

---

<sup>21</sup> This action acknowledged the vital role intelligence plays in combating terrorism—a fact clearly recognized by the 9/11 and WMD commissions—but still reflected the IRTPA direction that the Program Manager was “responsible for information sharing across the Federal Government.” Consequently, it was clear that the building the ISE was an effort that could not be accomplished within a single agency, but would have to be accomplished as a part of the larger interagency process.

<sup>22</sup> These functions include, among other things, the responsibility to “determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.” The President’s memorandum also required the DNI to ensure that the PM-ISE would be the assistant to the DNI in carrying out the functions delegated under the memorandum. In response to the April 10 Presidential direction, the DNI issued a memorandum on May 2, 2007 in

assigned to the DNI who was to perform them “in a manner consistent with the direction and guidance of the President.”

At the implementation level, the 2006 Implementation Plan states that it is the job of the PM-ISE to assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency, and policy compliance; and to regularly report the findings to Congress. Under the Bush administration, the PM-ISE was responsible for planning, oversight of implementation, and management of the ISE. In that capacity, he was advised by an interagency body—the Information Sharing Council (ISC).<sup>23</sup> In the event that the ISC was unable to reach agreement on an issue, the PM-ISE could, if necessary, submit that issue to an interagency policy coordination committee and perhaps even to the Homeland Security Council for resolution.

Both the President and the PM-ISE are advised by a Privacy and Civil Liberties Oversight Board.

Thomas E. McNamara, PM-ISE from 2006 until August 2009, identified the major challenges to improving interagency information-sharing to be changing the cultures, policies and business processes of the agencies.<sup>24</sup> In connection with that observation, he recommended the following three improvements: Establishment of a single national executive within the Executive Office of the President with budget certification authority to require agencies to build the ISE; single committee oversight of the ISE by both houses of Congress; and Presidential engagement of Cabinet officers in ISE matters.

Shortly after he took office President Obama issued Presidential Study Directive 1, which called for an interagency review of the White House homeland security and counter-terrorism structure. As a result, the President, on May 26, 2009, announced the integration of White House staff supporting national and homeland security into a single National Security Staff (NSS). The NSS supports all White House policymaking activities relating to international, transnational, and

---

which he charged the PM-ISE “with carrying out all responsibilities assigned to me by the President’s memorandum to ensure successful implementation of the Information Sharing Environment (ISE).”

<sup>23</sup>The Information Sharing Council (ISC), is made up of designees of the following departments and agencies: State, Treasury, Defense, Commerce, Energy, and Homeland Security; the Attorney General; the DNI; the Director of the Central Intelligence Agency; the Director of OMB ; the Director of the Federal Bureau of Investigation (FBI); the Director of the NCTC; and other heads of Federal departments or agencies as the DNI may designate. The ISC advises the President and PM-ISE on developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE. The ISE has a substructure of committees, working groups, and experts including two standing committees: a State, Local, and Tribal Subcommittee, and a Private Sector Subcommittee.

<sup>24</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/31/AR2009123101741.html>.

homeland security matters. Both the National and Homeland Security Councils continue to function, but they are supported by one integrated White House staff.

On July 2, 2009, the Assistant to the President for Homeland Security and Counterterrorism issued a memorandum to Federal agencies entitled “Strengthening Information Sharing and Access.” This memorandum established:

- a. The position of Senior Director for Information Sharing Policy in the Executive Office of the President; and
- b. An Information Sharing and Access (ISA) Interagency Policy Committee (IPC) to be chaired by the Senior Director.

Pertinent to PM-ISE, in an effort to streamline the process the ISC was integrated into the White House policy process through the ISA IPC. The ISA IPC has several subordinate bodies including the Senior Level Interagency Advisory Group (SLIAG), the ISE Privacy Guidelines Committee, and the Information Sharing Standards and Architecture Sub-IPC.