

FAA Telecommunication Infrastructure Review Panel

Phase 2 Report

Federal Aviation Administration

Washington, D.C.

June 2010

Version 1.0

FAA Telecommunication Infrastructure Review Panel

Phase 2 Report

Federal Aviation Administration

Washington, D.C.

June, 2010

Acknowledgements

The FTI Review Panel wishes to acknowledge the efforts of the many people who assisted us in conducting our Review. These include:

- Ms. Sandra Anderson, Project Manger, Data Communications NextGen Support (DataComm), FAA;
- Mr. Ahmad Usmani, Project Manager, System Wide Information Management (SWIM), FAA;
- Mr. Grant Miller and Mr. George Strawn, The Networking and Information Technology, Research and Development Program, Executive Office of the President;
- Dr. Chris Greer, Office of Science and Technology Policy, Executive Office of the President;
- Mr. Amit Yoran, CEO, Netwitness, Inc., former Director of US-CERT and National Cyber Security Division, Department of Homeland Security;
- Mr. Norm Laudermilch, Operations VP, TerreMark Corporation;
- Mr. David Barak, ATT Corporation;
- Mr. John Kefalitis, ITT Corporation;
- Mr. Thomas McNamara, Applied Physics Laboratory, The Johns Hopkins University, and
- Mr. Mark Fabbi, Vice President and Distinguished Analyst, Gartner, Inc.

whose willingness to cooperate, provide data and insights, host our site visits and answer our questions were greatly appreciated.

Washington, D.C.
June 30, 2010

Review Panel Approval

DAVE BOWEN
Assistant Administrator for Information Services and Chief Information Officer
Federal Aviation Administration

NANCY BROWN
Former Director of Command, Control, Communications and Computer Systems, Joint Staff; Vice Admiral, United States Navy (Ret.)

ANEESH CHOPRA
Assistant to the President and Chief Technology Officer
Office of Science and Technology Policy, Executive of the President

STEVE COOPER
Air Traffic Control Organization Chief Information Officer
Air Traffic Control Organization
Federal Aviation Administration

AMR ELSAWY
President and Chief Executive Officer
Member, Board of Trustees
Noblis

PATRICIA MCNALL
Assistant Chief Counsel
Acquisition and Commercial Law Division
Federal Aviation Administration

NITIN PRADHAN
Chief Information Officer
Office of the Secretary
Department of Transportation

FAA Telecommunication Infrastructure Review Panel

Phase 2 Report

Table of Contents

Executive Summary..... 5

Background..... 8

Panel Composition..... 9

Panel Objectives..... 9

Panel Activities..... 10

Panel Recommendations and Observations..... 12

Appendices..... 17

- Appendix I, Recommendation and Operating Principle Correlation
- Appendix II, Panel Biographies

Executive Summary

This is the second of two reports by the FAA Telecommunications Infrastructure (FTI) Review Panel (the Panel), commissioned by the FAA Administrator, to address a serious telecommunications outage of the FTI network on November 19, 2009. The first report, completed on April 20 2010, dealt with the outage itself; causes, factors, remediations, and made recommendations for actions to prevent a reoccurrence. This report deals with the broader issue of the reliability of contractor-provided Internet Protocol (IP) based networks such as FTI, to carry the critical navigation, communications and other data which will result from the implementation of the FAA's Next Generation Air Transportation System ("NextGen"), as well as recommendations to improve FAA's oversight of these networks.

While the first Phase of the Panel's work, reporting on the FTI outage, was relatively straightforward, the Panel found the work comprising the second Phase to be much more challenging. Not only was the scope of the investigation much more broad, but NextGen is an evolving program. These findings cut across many FAA areas such as organization, governance, processes and procedures, and others. In some cases, these recommendations involve changing FAA processes and organizational roles that have evolved over many years.

As the FAA transitions and implements NextGen, more of the systems and networks will become interconnected and network services will be provided by multiple vendors or service providers. Information sharing, interoperability, and collaboration requirements will increase, as will the complexity of the enterprise. The ability of the FAA to effectively manage its operations will become increasingly dependent on the quality and timeliness of information exchange. Requirements for increased governance, cyber security, situational awareness, interoperability, resilience, and operational efficiency must be redefined with an enterprise view. This will neither be easy nor quick. FAA governance structures, processes, resources and incentives must be re-evaluated to create the desired alignment around enterprise level requirements.

The fundamental issue addressed by this report is whether or not the planned increased utilization of IP-based network technologies is appropriate for use by the FAA as it transitions its current Air Traffic Control system to the "NextGen" systems, and employs new, digital technologies.

In the opinion of the Panel, the use of private IP-based networks as a foundational technology for NextGen is appropriate for meeting current and future functionality requirements and warranted from a cost management perspective. Such networks offer greater resilience, increased capacity, greater flexibility and greater adaptability than previous network solutions. By employing private networks, state-of-the-art tools and rigorous management and operational disciplines, such networks can be sufficiently secured and managed to meet the mission-critical needs of the FAA, whether operated by the FAA or by a contractor. This opinion represents the best thinking of industry and government experts. Similar strategies are being implemented by other major government agencies.

The Panel developed a set of Principles for effective management of mission-critical networks, based on discussions with government and industry experts. Those principles, which should be adopted by the FAA in maturing its network management processes, are as follows:

1. *The FAA must have end-to-end situational awareness of its network, integrated at a single location, for rapid understanding and event response;*

2. *The FAA must have end-to-end cyber security protection for its network, integrated into a single organization, for rapid understanding and event response;*

3. *Mission-critical components of the FAA network should be segregated from non mission-critical components and from the Internet;*

4. *Network connectivity standards should be developed and by policy, implemented by all FAA programs;*

5. *Key program services, such as cyber security protection, identity management and network connectivity should be standardized and provided to all programs in a uniform manner;*

6. *End-to-end resiliency must be designed into all FAA mission-critical programs, and*

7. *Governance must address requested changes to mission-critical program requirements.*

A correlation matrix between the Operating Principles and the Recommendations summarized below is shown in Appendix I.

This report makes the following recommendations for the FAA to consider in improving its programs and the oversight and operation of IP-based networks. These recommendations fall into the areas of Governance, Cyber Security, Situational Awareness, Interoperability, Resilience and Operational Efficiency.

The panel intends these recommendations to apply to all FAA programs and IP networks

1. Develop and implement a strategy to coordinate the FAA's network resources, with a single enterprise-wide view.

2. Develop mechanisms for seeking and incorporating FAA network user input on future requirements, quality of service provided and implementation priorities.

3. Expand the role of current FAA governance organizations and processes to provide an oversight role in implementation and operational phases of programs.

4. Implement an integrated end-to-end situational awareness capability across appropriate systems.

5. Redefine and enhance the Network Enterprise Management Centers (NEMC) to be the focal point for all Local Area Network (LAN) and Wide Area Network (WAN) visibility.

6. Increase FAA participation in advanced network technology groups both within and outside of government.

7. Expand the scope of cyber security detection and prevention services provided by the FAA's Cyber Security Management Center (CSMC) to all FAA systems.

8. Centralize the development of enterprise cyber security standards for operational systems, including a method for evaluating risk and determining the level of security required.

9. Include funding for an appropriate cyber security infrastructure in each NextGen program budget.

10. Devote funding for the development and implementation of a strategy to define and address the Agency's future staff skill set needs in the area of cyber security, networking, and other NextGen related technologies.

11. Add an independent verification capability and process to ensure comprehensive program compliance with cyber security standards.

12. Determine and assign specific organizational responsibility within the FAA to ensure that network connectivity is appropriately standardized and access to the network rigorously defined and monitored. Standardization includes the requirement to ensure that data flowing among all the FAA networks are appropriately interoperable.

13. Require that commercial service providers incorporate back-up sites that function as part of everyday operations, not just on stand-by in case of emergency .

14. Understand and mitigate network outage risks as appropriate for the service being delivered and its importance to both internal and external stakeholders.

Background

On November 19, 2009, maintenance work to replace and upgrade a network routing device in the FAA's FTI network caused a bottleneck in the network and resulted in a loss of communication across certain portions of the network from 5:10 AM Eastern time to 8:59 AM, nearly 4 hours. The FTI network is provided to the FAA through a contract with the Harris Corporation, of Melbourne, Florida. While there were a variety of FAA services affected, air traffic control radar and communication with aircraft were not affected and critical safety systems remained operational; safety of the flying public was never impacted. The most notable impact to the flying public was the inability of the FAA to receive flight plans via the FTI network. As a result, these flight plans had to be entered into the FAA air traffic control systems manually, causing the delay of over 800 flights that morning.

Flight delays have been an item of heightened concern by the flying public as the Nation's airspace has become more congested over the last several years. Disruptions due to weather and congestion at certain airports such as JFK, Chicago O'Hare, Atlanta, and Newark have had an effect of rippling through the air traffic system and causing delays across the country. While some disruptions are unavoidable, disruptions caused by equipment breakdowns are regarded as avoidable and put into question the FAA's ability to manage the current air traffic system while migrating to NextGen.

As a result of the November 19th communication outage, the Chairman of the House Transportation and Infrastructure Committee, Representative Oberstar (D., Minn.) and the Chairman of the House Subcommittee on Aviation, Representative Costello (D., Ill.) have called upon the Inspector General of the Department of Transportation to investigate the Harris Corporation's provision of services to the FAA, in a letter that reads in part:

> "Given the recent outage and its cascading effects, we request that your office undertake a 60-day study to examine the causes of the problem and whether FAA's corrective action plan will prevent future problems. Also, we ask that you examine FAA's ability to conduct oversight of FTI, and the implications for other critical modernization systems that will not be owned or operated by the Federal Government, such as the FAA's Automatic Dependent Surveillance - Broadcast satellite-based surveillance system."

In order to assure that all appropriate steps are taken to avoid similar disruptions in air travel, FAA Administrator J. Randolph Babbitt chartered a panel of experts (the "Panel") from both within and outside of the FAA to look into the outage and review the provision of services by FAA mission-critical service providers (the "Review").

The Panel was chartered to provide two reports: a report on the causes of the November 19th outage, with recommendations for preventing a reoccurrence, and a report on the suitability of contractor-provided Internet Protocol ("IP") based networks such as FTI, to support an increasing number of mission-critical services as NextGen is implemented.

This report details the findings of the second phase of the Panel's work, which consists of an assessment of the suitability of service provider-based IP networks and their use for National Airspace System ("NAS") operations. The report also includes recommendations, based on industry and government "best practices" for the organization, operation and oversight of these networks by the FAA.

Panel Composition

The Panel chartered by Administrator Babbitt is comprised of the following members:

- David Bowen – Chief information Officer, Federal Aviation Administration;
- Nancy Brown – Former Director of Command, Control, Communications and Computer Systems, Joint Staff; Vice Admiral, United States Navy (Ret.);
- Aneesh Chopra – Assistant to the President and Chief Technology Officer, Office of Science and Technology Policy, Executive Office of the President;
- Steven Cooper – Chief Information Officer, Air Traffic Organization, Federal Aviation Administration;
- Amr ElSawy – President and CEO, Noblis;
- Patricia McNall – Assistant Chief Counsel – Federal Aviation Administration, and
- Nitin Pradhan – Chief Information Officer, US Department of Transportation.

Biographies of the Panel members are shown in Appendix II.

Panel Objectives

The Panel's Review had the following objectives. Phase I report objectives included the following:

- Determine the root cause(s) of the outage of November 19, 2009;
- Determine if the Harris Corporation, in providing the FTI, has the adequate people, processes and technology deployed to provide a robust communications network, with adequate security, backup and fail-over capabilities, to meet the needs of the FAA;
- Determine the degree to which the Harris Corporation is using industry best practices in the architectural design, management and operation of the FTI, and if necessary, make suggestions for improvements;
- Assess the maturity of the processes and technology used within the Air Traffic Organization to monitor and oversee FTI, and make suggestions for improvements, and
- Determine the degree to which the FAA is using industry best practices to manage FTI, and make suggestions for improvements.

The objective of this Phase 2 report was primarily to:

- Determine the degree to which findings from this Review are relevant for the provision of other critical networking services to the FAA and as appropriate, recommend their adoption by other critical service providers.

Panel Activities

The Panel conducted the following activities in order to meet the objectives of the Phase 2 Report:

- Reviewed networking architecture and operating and security assumptions of major FAA NextGen programs such as System Wide Information Management (SWIM), Data Comm, and Automated Dependent Surveillance Broadcasting (ADS-B);
- Reviewed 'lessons learned" from the implementation of the Navy Marine Corps Internet (NMCI) infrastructure replacement program;
- Reviewed industry "best practices" in the areas of network management, mission-critical infrastructure operation, IT security and other areas. Sources of industry "best practices" came from interviews and operational reviews with the following organizations and individuals:
    - ITT Corporation
    - United States Navy
    - Johns Hopkins Research Laboratory
    - Terremark Worldwide Inc.
    - The Networking and Information Technology, Research and Development Program, Executive Office of the President
    - Mr. Amit Yoran
    - Mr. Mark Fabbi
- Evaluated the processes used by the ITT Corporation to manage and make changes to the ADS-B network, the degree to which they are consistent with industry best practices, and the degree to which they are followed by ITT and FAA Air Traffic Organization (ATO) personnel;
- Evaluated the ADS-B security and staff training programs, and
- Evaluated the processes used by the FAA to provide oversight to the ITT Corporation in maintaining ADS-B, and the degree to which they are consistent with industry best practices.

In addition, the Panel developed a set of Principles for effective management of mission-critical networks, based on discussions with government and industry experts. Those principles, which should be adopted by the FAA in maturing its network management processes, are as follows:

1. *The FAA must have end-to-end situational awareness of its network, integrated at a single location, for rapid understanding and event response.*

   Discussion: Situational information must be made easily accessible and available to the various monitoring centers that are responsible for stakeholder service, communications, and restoration of services. The FAA must maintain situational awareness regardless of how the service is being provided.

2. *The FAA must have end-to-end cyber security protection for its network, integrated into a single organization, for rapid understanding and event response.*

   Discussion: Sophisticated attacks can occur at any time and involve multiple locations, organizations, or providers. The key to rapid detection, protection and defense is a strong Cyber Security capability within the FAA. The FAA has state of the art facilities and capabilities that must be used more broadly, more consistently and more effectively. A key challenge is to build the trained workforce that can effectively steward the FAA services and oversee services provided by the vendors.

3. *Mission-critical components of the FAA network should be segregated from non mission-critical components and from the Internet.*

   Discussion: The FAA should maintain its reliance on "virtual private IP networks" as a way to manage service levels, security risks, network restoration of services, and recovery priorities, and maintain isolation from the Internet.

4. *Network connectivity standards should be developed and by policy, implemented by all FAA programs.*

   Discussion: The FAA has established a strong Enterprise Architecture and System Engineering development and governance structure that must continue to be engaged as programs move from one phase of their life cycle to the next. Configuration management and change control discipline must be applied to program plans, requirements, specification, and implementations to ensure the integrity of the systems evolution process.

5. *Key program services, such as cyber security protection, identity management and network connectivity should be standardized and provided to all programs in a uniform manner.*

6. *End-to-end resiliency must be designed into all FAA mission-critical programs.*

7. *Governance must address requested changes to mission-critical program requirements.*

A correlation matrix between the Operating Principles and the Recommendations that follow is shown in Appendix 1.

Recommendations and Observations

The Panel had observations in many areas that it found applicable to its Phase 2 tasking. For purposes of this report, the panel used the following descriptions of each area in this report:

- Governance – the process by which decisions regarding FAA systems are made;
- Interoperability – information flowing seamlessly among systems and stakeholders, both internal and external;
- Cyber Security – the detection, protection, scalability and speed of response when impacted by an adverse action;
- Situational Awareness – Continuously monitoring of FAA networks getting the right information to all involved parties in a timely fashion, and
- Resilience – the ability of a network to withstand negative events and continue operating.

This report makes the following recommendations for the FAA to consider in improving its programs and the oversight and operation of IP-based networks. These recommendations fall into the areas of Governance, Cyber Security, Situational Awareness, Interoperability, Resilience and Operational Efficiency.

The panel intends these recommendations to apply to all FAA programs and IP networks

Governance

Recommendation 1: Develop and implement a strategy to coordinate the FAA's network resources, with a single enterprise-wide view.

Observations:

- Information management is a core competency for the FAA;
- Best practices use centralized management of the network as a means to strengthen security through standardization;
- Multiple organizations oversee various components of FAA networking landscape, including vision setting, planning, implementation, operation and oversight;
- The complexities of operating in an all-IP network demand a more coordinated approach;
- The all-IP environment is so interwoven that any change could have a cascading effect and must be overseen by a central authority to ensure that the effect of unintended consequences are minimized, and
- True efficiencies can only be realized through consolidation

Recommendation 2: Develop mechanisms for seeking and incorporating FAA network user input on future requirements, quality of service provided and implementation priorities.

Observations:

- The formal interaction process between network services operators and users of network services could be significantly improved, and
- Governance processes in place at the FAA are primarily program centric rather than network centric.

Recommendation 3: Expand the role of current FAA governance organizations and processes to provide an oversight role in implementation and operational phases of programs.

Observations:

- Programs sometimes make changes without a full understanding of how those changes impact cost and schedule, or how they might impact other programs;
- Governance organizations can significantly improve programmatic reviews and investment decisions by increasing emphasis on cyber security, situational awareness, interoperability, and resilience;
- Although program managers do return to a governance organization for approval when deviating from approved scope or requirements, additional emphasis should be placed on returning when cost or schedule slippage is anticipated, and
- Program changes should be evaluated and signed off by the appropriate Enterprise Architecture board to ensure that the changes and their impact are incorporated into the FAA's Enterprise Architecture.

Situational Awareness

Recommendation 4: Implement an integrated end-to-end situational awareness capability across appropriate systems.

Observations:

- There is no common end-to-end view across all systems;
- There is no common language to promote understanding of situation and business impact;
- Restoration time is inversely proportional to amount of information shared, and
- True end-to-end situational awareness will greatly increase the speed at which decisions can be made.

Recommendation 5: Redefine and enhance the Network Enterprise Management Centers (NEMC) to be the focal point for all Local Area Network (LAN) and Wide Area Network (WAN) visibility.

Observations:

- NEMC is beginning to take this role on now, and has links established to the FTI WAN;

- A 60, 90 and 180 day plan should be developed to get visibility into information at service delivery points (SDP);
- There is no common view across all systems;
- True end-to-end situational awareness will greatly increase the speed at which decisions can be made, and
- NEMC currently has insufficient staff with the required skill sets, additional training will be required.

Recommendation 6: Increase FAA participation in advanced network technology groups both within and outside of government.

Observations:
- FAA can no longer depend merely on provider service levels and associated performance penalties as a means of continually improving service provider performance;
- Groups such as the Large System Networking area of the Networking Infrastructure Research and Development Program (NITRD) and its Joint Engineering Team ("JET") subgroup have much to offer in advancing "best practices" in network management. Consider adopting NITRD principles and tools developed by NITRD participants;
- Service providers respond well when incented by FAA, through contract provisions, to improve their capabilities and performance;
- FAA cannot leave it to service providers to be aware of and implement performance improvements on their own; the agency must be knowledgeable in new practices and tools and encourage their adoption by its service providers, and
- FAA must be capable of training and adopting its workforce to obtain the skills necessary to effectively carry out this recommendation.

Cyber Security

Recommendation 7: Expand the scope of cyber security detection and prevention services provided by the FAA's Cyber Security Management Center (CSMC) to all FAA systems.

Observations:
- While individual network components have their own security, no one has overall network security responsibility;
- Best practices require active collaboration among cyber security, network, and operational personnel;
- The CSMC has the people, processes, technology, inter-agency communications and inter-agency relationships that are critical to maintain awareness of outside threats. The CSMC is an excellent FAA resource;
- Cyber event detection capability is now more important to be within a network than to be merely at the boundaries, this enables end-to-end network security awareness;
- Defense in depth or layered defense can only be achieved through an enterprise-wide approach;
- Currently, CSMC services are limited to detection and notification. Best practices also include prevention services;

- Risk accepted on behalf of others without their knowledge has a cascading effect which is reduced by common standards and centralized control, and
- The use of commercial telecommunication service providers means there is no absolute guarantee of network segregation.

Recommendation 8: Centralize the development of enterprise cyber security standards for operational systems, including a method for evaluating risk and determining the level of security required.

Observations:
- Programs take varying approaches to security;
- Program contracts contain varying degrees of language relating to cyber security;
- The Internet, with moderate security, could be used for disseminating information to external users, and
- The FAA has operational requirements that are mission-critical and the Internet cannot be sufficiently secured at this time to provide the required level of protection.

Recommendation 9: Include funding for an appropriate cyber security infrastructure in each NextGen program budget.

Observations:
- Programs are unsure of what they're spending on security;
- Programs take varying approaches to security;
- Cyber security for each NextGen program is not standardized, nor does it use a common security infrastructure, and
- Current varied infrastructures do not enable a rapid response to insider and outsider threats.

Recommendation 10: Devote funding for the development and implementation of a strategy to define and address the Agency's future staff skill set needs in the area of cyber security, networking, and other NextGen related technologies

Observations:
- The Agency has adequate work plans in place to address future Acquisition, system engineering, air traffic controller and aviation inspector need;
- NextGen programs and technologies require strong FAA leadership and technical competence to effectively manage the NextGen portfolio of program;
- Competition for these skill sets is intense across both the government and private sectors, and
- This skill set acquisition plan should be monitored as the FAA is currently doing with its other critical skill set positions.

Recommendation 11: Add an independent verification capability and process to ensure comprehensive program compliance with cyber security standards.

Observations:
- That function does not exist today, and
- No single individual has overall security responsibility for the FAA networks.

Interoperability

Recommendation 12: Determine and assign specific organizational responsibility within the FAA to ensure that network connectivity is appropriately standardized and access to the network rigorously defined and monitored. Standardization includes the requirement to ensure that data flowing among all the FAA networks are appropriately interoperable.

Observations:

- FAA organizations are producing multiple networks; FAA has no assurance that data flowing across these networks is interoperable. These practices can add risk cost and vulnerabilities to the operations;
- There are no standards for network connectivity, and
- Different FAA programs and organizations use different network connectivity architecture.

Resilience

Recommendation 13: Evaluate which NextGen critical services require a hot back up site that is geographically diverse from the warm site, and are not just on stand-by in case of emergency.

Observations:

- Back up sites for some critical services are not geographically diverse;
- Service provider continuity of operations (COOP) plans are not tightly coupled to an overall FAA COOP plan, and
- For some critical services, restoration and recovery requirements preclude sole reliance on a cold back up site.

Recommendation 14: Understand and mitigate network outage risks as appropriate for the service being delivered and its importance to both internal and external stakeholders.

Observations:

- Network providers can provide varying service levels to meet the needs of the systems using them;
- Best Practice dictates that stakeholders are notified of service outages and recovery plans and that the Agency understands the impact of an outage to the stakeholders;
- There was a mismatch between the level of service provided, and the stakeholders expectations, and
- Preplanned recovery and communication strategies increase in importance as network complexity increases.

A correlation matrix between the Operating Principles and Recommendations is shown in Appendix 1.

Appendices

Appendix I - Recommendation/Operating Principle Correlation

Appendix II - Panel Member Biographies

Appendix I

FTI Recommendation and Operating Principle Correlation

Principles / Recommendations	End-to-End Situational Awareness	End-to-End Cyber Security Protection	Segregate Mission and non-Mission Critical Components	Implement Network Connectivity Standards	Standardize Key Program Services	Ensure End-to-End Resiliency	Govern Changing Requirements.
1 - Consolidate Network Management Resources	X					X	
2 - Involve Users in Network Service Governance	X						X
3 - Govern Changing Operational Program Requirements	X						X
4 - Implement End-to-End Situational Awareness	X	X		X	X	X	
5 - Enhance NEMC to be Focal Point for LAN and WAN Visibility	X	X			X	X	X
6 - Be Proactive in Joining Advanced Technology Groups	X	X				X	
7 - Extend Cyber Security Services to the NAS	X	X			X		
8 - Certify That Cyber Security Standards Are Being Met		X			X	X	X
9 - Budget for Common Cyber Security Infrastructure	X	X			X	X	X
10 – Funding for Development and Strategy of Future Skill Sets	X	X	X	X	X	X	X
11 - Centralize Development of Cyber Security Standards		X			X	X	X
12 - Standardize Network Connectivity Specifications	X	X	X	X	X	X	
13 - Ensure Backup Sites Participate in Operations						X	
14 - Understand and mitigate network outage risks	X		X	X		X	

Appendix II – Panel Member Biographies

DAVE BOWEN
Assistant Administrator for Information Services and Chief Information Officer
Federal Aviation Administration

Dave Bowen is the Federal Aviation Administration's (FAA) Assistant Administrator for Information Services and Chief Information Officer (CIO). Bowen is responsible for developing, structuring, implementing, and communicating policy and practice as it pertains to the Agency's information technology (IT) investment, management, planning, research and development, and security. In 2009, he was recognized by 'Information Week' as one of the top 50 CIO's in state, local and federal government.

Prior to joining the FAA in February 2006, Bowen spent more than 25 years in healthcare IT management in the provider, payer, consultant, and vendor areas. He most recently served as the Senior Vice President for IT and CIO at Blue Shield of California, a $6.2 billion health plan with more than 2.5 million members. Blue Shield is the second largest not-for-profit healthcare organization in California. While there, Bowen directed Blue Shield's IT, telecommunication, business recovery, and Web implementation resources with an operating budget in excess of $100 million. He sat on Blue Shield's Operations Committee and its Senior Staff.

Prior to Blue Shield, Bowen was Senior Vice President for Information Management and CIO of Catholic Healthcare West (CHW), the fifth largest healthcare delivery system in the United States. His responsibilities included oversight of CHW's Information Management and Telecommunications resources located throughout Arizona, California, and Nevada. He also managed CHW's Year 2000 initiative.

Bowen has also served as the Senior Vice President for Information Systems and CIO at Baptist Health System, Inc., of Birmingham, Ala., a 13-hospital system and the largest integrated healthcare delivery system in Alabama. In addition, he was CIO of its wholly-owned Health Maintenance Organization, Health Partners of Alabama.

He is the former Board Chairman of the Coastside Family Medical Center, former Chairman of the Blue Cross Blue Shield Association IT Roundtable, and member of the Blue Cross Blue Shield Association Interplan Technology Advisory Council.

Bowen has an undergraduate degree in economics from Ursinus College, Collegeville, Pa., and a master's degree in business with distinction from the Johnson Graduate School of Business, Cornell University, Ithaca, N.Y. He is also a CPA, holds an FAA Commercial Pilot certificate, and has more than 30 years of flying experience.

Appendix II – Panel Member Biographies

NANCY E. BROWN
Former Director of Command, Control, Communications and Computer Systems, Joint Staff; Vice Admiral, United States Navy (Ret.)

After completing over 35 years of service Vice Admiral Nancy E. Brown retired from her position as the Director, Command, Control, Communications and Computer Systems, The Joint Staff. Since retiring on 1 October 2009, she has been nominated to serve as an Outside Director of Systematic Software and on the Board of Directors of the United States Naval Institute. She has accepted consulting opportunities with Cypress International and IZ Technologies.

While on active duty her command tours included an assignment as Officer in Charge, Naval Radio and Receiving Facility Kami Seya, Japan, Commanding Officer of the Naval Computer and Telecommunications Station Cutler, Downeast, Maine and Commanding Officer Naval Computer and Telecommunications Area Master Station Atlantic, Norfolk. She was on the National Security Council staff at the White House and was also the Deputy Director, White House Military Office. In August 2004 she deployed to Iraq becoming the first Multi-National Force–Iraq C6 headquartered in Baghdad. Returning in April 2005 she was assigned as the J6 for both North American Aerospace Defense Command and United States Northern Command. In August 2006 she assumed her last active duty position as the Director, Command, Control, Communications and Computer Systems (C4 Systems), The Joint Staff.

Vice Admiral Brown's decorations include the Defense Distinguished Service Medal (with Oak Leaf Cluster), the Defense Superior Service Medal (with two Oak Leaf Clusters), the Legion of Merit (with Gold Star), the Bronze Star Medal, the Defense Meritorious Service Medal (with Oak Leaf Cluster), the Meritorious Service Medal, the Navy and Marine Corps Commendation Medal, the Navy and Marine Corps Achievement Medal, the Iraq Campaign Medal (with two Bronze Stars), the Global War on Terrorism Medal, the Armed Forces Service Medal, and the National Defense Service Medal (with two Bronze Stars).

ANEESH CHOPRA
Assistant to the President and Chief Technology Officer
Office of Science and Technology Policy, Executive of the President

Aneesh Chopra is the Chief Technology Officer and Associate Director for Technology in the White House Office of Science & Technology Policy. He was sworn in on May 22, 2009. Prior to his appointment, he served as Secretary of Technology for the Commonwealth of Virginia from January 2006 until April 2009. He previously served as Managing Director with the Advisory Board Company, a publicly-traded healthcare think tank. Chopra was named to Government Technology magazine's Top 25 in their Doers, Dreamers, and Drivers issue in 2008. Aneesh Chopra received his B.A. from The Johns Hopkins University and his M.P.P. from Harvard's Kennedy School. He and his wife Rohini have two young children.

Appendix II – Panel Member Biographies

STEVE COOPER
Air Traffic Control Organization Chief Information Officer
Air Traffic Control Organization
Federal Aviation Administration

Steven I. Cooper is a founding partner of Strativest (www.strativest.com), a firm focused on identifying emerging technologies applicable to homeland security and emergency response and preparedness, assisting in the development of 'go-to-market' actions, and in providing management advisory services for business strategy and business development, competitive intelligence, and the strategic use of information and communications technology for competitive advantage.

In November 2007, Mr. Cooper joined Fortified Holdings Corporation (www.fortifiedholdings.com) as President. Fortified Holdings is a diversified holding company focused on the development and delivery of solutions to improve situational awareness across the homeland security and first responder communities. In addition to operational responsibilities, he is focused on identifying acquisition targets for the company and helping its business units expand their market reach in effectively delivering its product solutions to emergency management organizations like the Federal Emergency Management Agency, local municipalities, first responders, and government and military agencies, to include the Department of Homeland Security, the US Army, and the US Coast Guard.

From May 2005 to July 2007, he was senior vice president and chief information officer (CIO) of the American Red Cross. Mr. Cooper was responsible for the information technology (IT) assets of the Red Cross and leveraging them to support the humanitarian organization's 35,000 employees and the 300 million Americans they serve. He guided the introduction of a first ever national call center during Hurricane Katrina to provide emergency assistance to the more than 4 Million people displaced from their homes and led the strategic sourcing of the ARC's primary data center.

In February 2003, he was appointed by President George W. Bush as the first CIO of the Department of Homeland Security (DHS). His accomplishments include the implementation of a Homeland Secure Data Network to enable the exchange of classified homeland security information among federal civilian agencies and with the Department of Defense; in partnership, with the Federal Bureau of Investigation (FBI), the deployment of a Homeland Security Information Network to share sensitive information with state and local agencies; first responders, and private sector entities who own critical infrastructure; in developing the department's first IT Strategic Plan, and in standing up the 'day one' IT operations of DHS. Mr. Cooper testified frequently before Congress on matters related to Cyber and Information Security, and the use of Information Technology to achieve homeland security mission objectives.

Earlier, in March 2002, Mr. Cooper was appointed Special Assistant to the President for Homeland Security and also served as senior director for information integration in the White House Office of Homeland Security. In this role, he initiated the integration of the terrorist watch lists, and launched the development of the National Enterprise Architecture for Homeland Security to address information integration within the federal government and the sharing of homeland security information with state, local, and relevant private-sector entities.

Mr. Cooper was named one of the Top 100 CIOs in America by CIO Insight in 2007. He previously was honored by Government Computer News as the Government Civilian Executive of the Year; by the Northern Virginia Technology Council as a Titan of Technology; was a recipient of the Fed 100 Award recognizing the 100 most influential people in Federal Government Technology; and was named by the Washington Post as One of the Five to Watch while serving in the White House.

Mr. Cooper has remained active in his support of the NGO and Not-for-profit sector. Continuing work he did with the Department of Homeland Security in public safety interoperability through his current role as a Board Member of ComCARE (www.comcare.org), he is currently participating in the ComCARE Alliance's Core Services Initiative to provide a nationwide Enterprise Provider Access Directory and Identity Management services for all members of the emergency response community.

As a Board Member of NetHope (www.nethope.org), he is working to extend Information and Communication Technology capability, infrastructure, and innovation across the globe on behalf of NetHope's members, the 23 largest global humanitarian organizations, to 'wire the global village'.

Mr Cooper serves as an executive board member of the National Institute for Urban Search and Rescue, and as a board member of AFCEA International, both not-for-profit organizations dedicated to addressing matters of disaster preparedness and national security at all levels of government and for each citizen and family.

As the first Executive-on-Grounds at the University of Virginia, McIntire School of Commerce, Mr. Cooper brings "real-life" experience in applying technology to the students in the Masters program in the Management of IT.
Prior to his federal government service, Mr. Cooper spent more than twenty years in the private sector as an IT professional and holds a BA degree from Ohio Wesleyan University. He is a former Naval Air Reserve petty officer who served during the Vietnam conflict. He is married and states that being the father of four daughters, and the brother of four sisters, remains the toughest job he's ever had.

Appendix II – Panel Member Biographies

AMR ELSAWY
President and Chief Executive Officer
Member, Board of Trustees
Noblis

As President and Chief Executive Officer, Mr. ElSawy is responsible for the general management and direction of the company's overall technical, financial, and administrative activities. Noblis is a nonprofit science, technology and strategy organization working at all levels of government, in private industry and with other nonprofits in areas that are essential to our nation's well being: national and homeland security, public safety, transportation, health care, criminal justice, energy and the environment, and oceans, atmosphere and space.

Mr. ElSawy was elected Executive Vice President and a member of the Board of Trustees of Noblis in January 2007. He has extensive experience leading organizations and developing innovative solutions to some of the most complex challenges in the public sector.

Prior to joining Noblis, Mr. ElSawy was Senior Vice President and General Manager of MITRE's domestic and international aviation and transportation security work program.

Mr. ElSawy established and ran public-private partnerships. He has earned an international reputation as a leader in aviation. His work experience includes research and development, complex systems engineering, modeling and simulation and informing domestic and international aviation policy.

In 2005, Mr. ElSawy was elected Vice President of Standards and a member of the board of AIAA. He served as Chairman of RTCA from 2004 – 2006, and was a member of the FAA Research and Development Committee (REDAC). He served as the director of the FAA FFRDC from 1999 – 2006.

Prior to 1997, Mr. ElSawy served in various senior management positions and was responsible for strategy development, cross-functional integration, systems engineering, and architecture evolution of programs. He also served as a member of executive panels responsible for oversight of the implementation of large distributed information systems and networks for the Jet Propulsion Laboratory (JPL) and the Advanced Weather Information Processing System of the National Weather Service (NWS).

Mr. ElSawy holds a master's degree in business administration from Georgetown University - 1998, a master's degree in electrical engineering from George Washington University - 1980, and a bachelor's degree in electrical engineering from West Virginia University - 1977. He was inducted in the Computer Science and Electrical Engineering Academy at WVU in 2007.

Appendix II – Panel Member Biographies

PATRICIA A. MCNALL
Assistant Chief Counsel
Acquisition and Commercial Law Division
Federal Aviation Administration

Since 1994, Ms. McNall has been the Assistant Chief Counsel for Acquisition and Commercial Law at FAA. In her 26-year FAA career, Ms. McNall's principal practice has been in the area of Government contracts, but she has served in various other positions, including Acting Deputy Assistant Administrator for Policy, Planning and International Aviation, Deputy Assistant Chief Counsel for FAA's Technical Center, Special Assistant to the Chief Counsel, and acting Deputy Director for the FAA's Office of Acquisitions. In 1995, Ms. McNall worked with a Blue Ribbon Panel of acquisition experts and attorneys to create a new acquisition management system for the FAA. In late 1993, she served as Co-Chair of the Budget and Finance Working Group as part of the Department of Transportation's initiative to create an Air Traffic Control Corporation. She has received numerous awards including a National Performance Review "Hammer" award from the Vice-President, the Federal Bar Association's Transportation Lawyer of the Year, the Secretary's "Gold Medal" award, Outstanding Attorney at FAA for the year, Logistics Service Award, Quality Action Team awards, and numerous Special Achievement Awards.

In 1985, Ms. McNall earned her J.D. from George Washington University. In 1982 she studied law, foreign trade and Chinese language through a Columbia University program held at the Shanghai Law Institute. She also holds a M.A. (1982) in Economics and International Relations from the Johns Hopkins University School of Advanced International Relations, and a B.A. (1979) in International Relations and Asian Studies from Scripps College.

Appendix II – Panel Member Biographies

NITIN PRADHAN
Chief Information Officer
Office of the Secretary
Department of Transportation

Mr. Nitin Pradhan was sworn in on July 6th, 2009 as the Departmental Chief Information Officer (CIO) for the US Department of Transportation (DOT) as part of the Obama administration. He is the chief advisor to Secretary Ray LaHood in all matters relating to information technology. In this role of the Departmental CIO, Mr. Pradhan provides information technology vision, strategy, planning, policy and oversight for DOT's $3.0+ billion IT portfolio.

Nitin is a business strategist, technology expert, coalition builder and change agent with over twenty years of experience including eleven years at CXO level in government, startups, non-profits and private industry. Nitin's expertise is in targeting new opportunities utilizing technology as a solution; advising operational managers in launching and promoting knowledge centric products and services; and defining fundamental organizational transformation integrating entrepreneurship, innovation, and technology, as well as institutional and partner knowledge. His current focus is on Enterprise 2.0 based communications, collaboration and community building, and information assurance, security and privacy. Nitin is also a strong proponent of building public-private partnerships. Nitin was recently named to Information Week's "Government CIO 50: Driving Change in the Public Sector" for bringing a business person's point of view to management of the DOT's IT strategy, policy and implementation.

Prior to joining DOT, Nitin was an IT Executive at Fairfax County Public Schools (FCPS), the 12th largest school district in USA. FCPS IT department has been ranked in the CIO Magazine's top 100 IT organizations and Computer World's 100 best places to work in the nation.

Prior to joining FCPS, Nitin was the Managing Director of Virginia's Center for Innovative Technology (CIT), where his targeted focus was on mentoring and growing technology startups and building research and innovation capabilities and capacity. He has also been the co-founder and interim CEO of a wireless startup.
Mr. Pradhan's educational qualifications include a BS degree in engineering and an MBA in marketing from India, as well as an MS in accounting from the Kogod College of Business at The American University, in Washington DC. He lives with his wife, son and daughter in Northern Virginia.