Net-Centric Operations Concept of Operations

Version 1.0 | July 7, 2010

Joint Planning and Development Office
Net-Centric Operations Division

Next Generation Air Transportation System
Joint Planning and Development Office

Table of Contents

EXECUTIVE SUMMARY ES-1

1 SCOPE 1-1

1.1 PURPOSE 1-1
1.2 DESCRIPTION 1-1
1.3 OVERVIEW 1-2

2 CURRENT OPERATIONS 2-1

2.1 BACKGROUND, OBJECTIVES AND SCOPE 2-1
2.2 OPERATIONAL POLICIES AND CONSTRAINTS 2-1
2.3 DESCRIPTION OF CURRENT OPERATIONS 2-3
2.4 MODES OF OPERATION FOR THE CURRENT SITUATION 2-6
2.5 USER CLASSES AND ORGANIZATIONS 2-7

3 JUSTIFICATION FOR AND NATURE OF CHANGES 3-1

3.1 JUSTIFICATION FOR CHANGES 3-1
3.2 DESCRIPTION OF DESIRED CHANGES 3-3
3.2.1 Drivers 3-4
3.2.2 Infrastructure 3-5
3.3 PRIORITIES AMONG CHANGES 3-6
3.4 CHANGES CONSIDERED BUT NOT INCLUDED 3-7
3.5 ASSUMPTIONS AND CONSTRAINTS 3-7

4 CONCEPTS FOR THE PROPOSED SYSTEM 4-1

4.1 BACKGROUND, OBJECTIVES, AND SCOPE 4-1
4.2 OPERATIONAL POLICIES AND CONSTRAINTS 4-1
4.3 DESCRIPTION OF PROPOSED ACTIVITIES AND OPERATIONS 4-3
4.3.1 Overview 4-3
4.3.2 Civil Aviation 4-4
4.3.3 Security and Law Enforcement 4-6
4.3.4 National Defense 4-8
4.4 MODES OF OPERATION FOR THE NEXTGEN ATS 4-9
4.5 USER CLASSES AND OTHER INVOLVED PERSONNEL 4-9
4.6 DEVELOPMENT AND SUPPORT ENVIRONMENT 4-9

5 OPERATIONAL SCENARIOS 5-1

6 SUMMARY OF IMPACTS 6-1

6.1 OPERATIONAL IMPACTS 6-1
6.1.1 Flow Management 6--2
6.1.2 Weather 6-2
6.1.3 Aviation Security 6--2
6.1.4 Environmental Management 6-3
6.2 ORGANIZATIONAL IMPACTS 6-3
6.3 IMPACTS DURING DEVELOPMENT 6-4

7 ANALYSIS OF THE PROPOSED SYSTEM 7-1

7.1 SUMMARY OF IMPROVEMENTS 7-1
7.2 DISADVANTAGES AND LIMITATIONS 7-2
7.3 ALTERNATIVES AND TRADE-OFFS CONSIDERED 7-4

DRAFT

APPENDIX A: DESCRIPTION OF CURRENT OPERATIONS BY MISSION AREA A-1

A.1 CIVIL AVIATION A-1
A.2 SECURITY AND LAW ENFORCEMENT A-4
A.3 NATIONAL DEFENSE A-5

APPENDIX B: USER OPERATIONS B-1

APPENDIX C: SCENARIOS C-1

APPENDIX D: ACRONYMS D-1

APPENDIX E: REFERENCES E-1

APPENDIX F: GLOSSARY F-1

DRAFT

Executive Summary

By 2025, the National Airspace System (NAS) will have seen a significant increase in the volume of air traffic that traverses its airways. Today's business processes and IT systems are not designed to accommodate such volume. Among the critical changes that today's NAS must undergo if it is to meet the demands of the Next Generation Air Transportation System (NextGen) is a change in the manner in which information is collected, processed, analyzed, displayed, and disseminated. NextGen users - from passengers traveling to vacation destinations to Air Traffic Controllers directing departures and landings at high-density airports to Air Force fighter pilots interdicting unauthorized aircraft trying to enter U.S. airspace - must have ready access to the up-to-date, reliable, authoritative information that is crucial to the success of their missions. In today's NAS, this information is hard to find, frequently inaccessible, and sometimes un-interpretable even when it can be found and accessed. As a result, situational awareness is less robust than it should be, collaboration is difficult to manage, and decision-making can be unnecessarily time-consuming, or must be done with inadequate or inaccurate information.

Net-centric Operations will be at the heart of the transformation from NAS to NextGen. As the volume of air traffic increases, terrorism remains a constant threat, and criminals continue to use the airways to carry out illegal activities, decision making in the NextGen era will become ever more complex and fast-paced. Almost every significant decision, and its execution, will require cooperation and coordination between multiple, geographically dispersed participants. Net-centric Information Exchange and Infrastructure Services that enable information producers to publish their information, and authorized consumers to access the information they need, when they need it, are key to creating a safe, efficient, and thriving Air Transportation System in which users enjoy ample, shared situational awareness in a collaborative environment.

In contrast to today's environment of isolated IT systems that exchange information by way of point-to-point connections, information resources and applications in the NextGen Service Oriented environment will be accessible on request to anticipated and unanticipated users alike. Ready access to data, together with semantically robust data reference models and service descriptions, will create an agile development environment in which application developers can quickly and easily design, build and test new and innovative applications for using the data available on the NextGen network. Programs to automate currently time-consuming or cumbersome processes such as trajectory planning or surveillance track resolution will be commonplace in the NextGen era. Like data services, software services will be available to any authorized consumer.

Net-centric operations and governance will facilitate new and more effective cyber security measures such as federated identity management, data provenance safeguards, and software certification programs, giving NextGen data consumers confidence in the integrity and reliability of the information they are receiving, and assuring NextGen data providers information of the confidentiality and security of the information they are disseminating. System security measures

DRAFT

will be implemented consistently across NextGen user communities, based on pre-established agreements about risk levels, and roles and permissions associated with networked information. NextGen Net-centric Operations governance authorities will help to establish a climate of trust between service consumers and service providers. Access to information and services within NextGen will require verification along multiple dimensions, including user identification, role specification, and information classification, providing the highest possible level of confidence that users are accessing only information to which they are entitled. Provision of information and services within NextGen will require certification along multiple dimensions, including data provenance, national security classification, encryption, key management, compliance with privacy protection and other laws. Standardized configuration and change management procedures will aid inter-organizational as well as *intra*-organizational consumers by ensuring that changes do not disenfranchise known users.

Ultimately, good information facilitates good decision making, and good decision making facilitates successful operations, whether by a passenger deciding which flight to book for a Hawaiian vacation, or by a Combat Commander deciding whether or not to shoot down a suspicious aircraft. In the NextGen environment, not only will it be possible to make decisions faster and more collaboratively, but the decision makers will be confident that the decisions they make are made with the most comprehensive, authoritative, and up-to-date information possible.

DRAFT

1 Scope

The successful implementation of the Next Generation Air Transportation System (NextGen) will transform air transportation in the United States, significantly improving international transportation of goods and people, efficiently accommodating increased demand, while minimizing environmental impacts. Realizing such a ground-breaking operational environment is dependent upon the creation of an advanced, net-centric communications system that will provide:

> (1) access by all NextGen users, according to their level of authorization and their particular roles, to the information they need to conduct their operations and make well-informed, timely decisions;
> (2) tools to organize, process, and present information in interactive displays that support (a) collaboration among geographically dispersed partners, and (b) real-time analysis, decision-making and action;
> (3) the ability to keep information secure, while ensuring access for authorized users.

Implementing this system will be a challenge that must be undertaken incrementally. This Net-centric Operations Concept of Operations (NCO ConOps) does not purport to be a technical implementation guide to Information Exchange Services (IX Services) within NextGen. Rather, the NCO ConOps presents a view, from the perspective of NextGen users, on how the system will operate and evolve, and how NextGen users will benefit once the infrastructure is in place to support the information sharing, shared situational awareness, and collaborative decision making that comprise the core objectives of NextGen.

1.1 Purpose

The NCO ConOps expands on the vision for Net-centric Operations set forth in Version 3.0, Chapter 4, of the Joint Planning and Development Office's (JPDO's) NextGen ConOps. It discusses, from an operational perspective, the IX Services envisioned in NextGen and emphasizes how NextGen IX Services will enable users to perform their roles more efficiently and effectively. This NCO ConOps should be used as guidance for the development of future roadmaps, requirements documents, and functional specifications for IX Services and supporting technologies.

1.2 Description

Focusing on three primary NAS mission areas – civil aviation, security and law enforcement operations, and national defense - and the architectural and engineering activities needed to support the exchange of information among NAS users responsible for carrying out those missions, the ConOps describes:

DRAFT

- the current state of information sharing and collaborative decision making within the National Airspace System (NAS), and the ways in which the current system constrains NAS operations, hinders innovation, and limits opportunities for growth;
- the net-centric capabilities and infrastructure requirements for addressing the shortcomings of the current system;
- the future-state vision for how NextGen users will leverage net-centric IX Services to accomplish their goals in the NextGen era;
- opportunities for developers to exploit net-centric IX Services to design and develop innovation applications for processing, analyzing, aggregating, correlating, and displaying data to meet user demand and drive additional improvements to NAS safety and efficiency; and
- the governance and oversight challenges that information sharing on the scale contemplated here will generate.

1.3 Overview

To meet the increase in air traffic anticipated by 2025 while maintaining the United States as the safest air transportation system in the world, NextGen must provide users - including air travelers, cargo shippers, airport planners, air and ground crews, Air Navigation Service Providers (ANSPs), safety and security operators, law enforcement officers, intelligence analysts, military personnel and others - the ability to engage in collaborative decision making in an environment that provides the appropriate shared situational awareness.

In accordance with their level of authorization, users will be able to access NextGen information from wherever they are, whether in the United States or abroad. Because some NextGen data will be completely unrestricted, while other data will have stringent proprietary or national security restrictions attached to it. User authentication will require a robust, integrated personal identity management system (PIMS) that can confidently assess a user's credentials upon log-in, recognize and defeat spoofers and hackers, and ensure that legitimate users can access all the information that their credentials support. The origin and rigor of credentials that will be accepted in the NextGen environment will vary by user type. For instance, passengers typically will have less rigorous credentials – and correspondingly less access to information – than government employees with high-level security clearances.

The management and presentation of data is as crucial to the NextGen vision as *access* to data. NextGen will need applications that can filter the information needed for decision making from the irrelevant information that creates information overload without improving situational awareness. Appropriate information will be accessible on request, or disseminated through publish-subscribe agreements, in a manner consistent with user roles and the decision-making processes associated with those roles. The information presented, for instance, to potential passengers making flight decisions for their vacation will be different from the information presented to Air Traffic Controllers making decisions about re-routing an aircraft around adverse weather. But in every case, the information presented will be from reliable, authoritative

DRAFT

sources, and be based on a consistent understanding of the data vocabulary and the intended use of the data.

NextGen Net-centric Operations will be made possible by the incremental implementation of a semantic, service-oriented infrastructure comprising a system of shared, reusable services that search for, access, process, disseminate, and display NextGen information. Metadata expressed in a standardized, machine-readable, formal language and describing NextGen information resources and services will facilitate a shared, consistent understanding of data vocabularies and enable state-of-the-art information discovery capabilities such as federated querying and semantic search. Communities of Interest (COIs) made up of NextGen data consumers and data producers from across the entire spectrum of NAS users will be responsible for creating and maintaining the semantic models of the information within their domain, and for producing the machine-readable documentation describing the services connected with the data. Such metadata can include information about the authority, timeliness, and security and privacy parameters of the data sources, and the content and context of the data they provide.

Net-centric Operations represent a fundamental shift at the technical, process, and organizational levels of the NAS. In the past, the various systems that help to run the NAS have been architected in isolation from one another, leading to redundant functionality and an inability to share information. In NextGen, these segregated architectures will be replaced by enterprise architectures, in which systems are designed and implemented as part of an integrated whole. Information produced by one system will be readily available to another. Processes will shift from a norm in which groups work in isolation, using organization-specific systems, to one in which collaboration across agencies, user classes, and sectors, is standard. Cumbersome and time-consuming information exchange procedures will be replaced by agile communications networks geared to solving mission-related problems by tapping into a shared pool of information resources and software services. The concept of Net-centric Operations encompasses the view that the overall mission is paramount, and stakeholders need to work in partnership for NextGen to succeed.

The NCO ConOps discusses NextGen operations in terms of the desired 2025 end-state for IX Services in the NextGen system of systems that connects public and private entities alike. However, it is understood that the achievement of this end-state will occur only through iterative and incremental development efforts that will transform the NAS from a system of stove-piped, legacy systems into a system of interoperable, reusable web-based services.

DRAFT

2 Current Operations

2.1 Background, Objectives and Scope

NAS usage encompasses a broad range of activities, including commercial air passenger travel, air cargo transport operations, general and recreational aviation, and security, law enforcement and defense operations. Accommodating this diversity of activities on the scale that it occurs within the NAS requires adaptive, sophisticated and well orchestrated communications and exchanges of information among a diverse and widely distributed community of users. Information exchanges must occur across multiple networks, and must ensure security at multiple levels, from publicly accessible data to top-secret government documents.

The description of current operations provided here attempts to give the reader a broad overview of the types of information that must be exchanged among the diverse classes of NAS users. The NCO ConOps focuses on three major NAS mission areas; Civil Aviation, Law Enforcement and Security, and National Defense. Operations within these mission areas are discussed in terms of the information exchanges that they engender, the barriers to growth, and the threats to safety and security that are posed by the lack of a flexible, extensible, and secure information exchange infrastructure. While the discussion in this section is necessarily high-level, appendices have been included that provide a more detailed discussion of each mission area. Moreover, the scenarios that are appended to this ConOps provide additional details about the information exchange requirements of the NAS, today and in the future.

2.2 Operational Policies and Constraints

The need for network-enabled information access throughout NextGen is well-documented in numerous directives, strategy documents, and briefings. The Vision 100 – Century of Aviation Reauthorization Act lists as goals: to "take advantage of data from emerging ground-based and space-based communications, navigation, and surveillance technologies;" and to "integrate 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." The President's National Strategy for Information Sharing, to name another example, notes that "information related to terrorism is derived by gathering, fusing, analyzing and evaluating relevant information from a broad array of sources…" The National Security Presidential Directive-47/Homeland Security Presidential Directive-16 (NSPD-47/HSPD-16), which directs the operational implementation of the National Strategy for Aviation Security (NSAS), notes that "information sharing enables all aspects of NSAS activity". The strategy calls for the development of technologies to promote information sharing among all levels of government and among government agencies and the public sectors.

The information exchange and automation services envisioned in the NextGen Integrated Work Plan (IWP) demand a net-centric environment in which NAS users from every sector can access, display, analyze, share, and disseminate information as appropriate to the individual user's roles, permissions, and security clearances. Today, however, the discovery, analysis and exchange of

DRAFT

information remain excessively cumbersome and inadequate for meeting the demands of tomorrow's air transportation needs. Within the Federal government agencies that bear responsibility for the safe, secure and efficient operation of the NAS, present day operations are predominantly conducted as if each agency is an enclave unto itself, with little system integration, information sharing, collaborative decision making, or shared situational awareness across agencies. In some cases, the reigning culture is even antithetical to information sharing. In most cases, there are few official policies, rules, or regulations to guide the exchange of information across agencies, and between the government, commercial, and private sectors. Policy regarding coordinated architecting and collaborative systems engineering among disparate government agencies has not been developed.

Often, existing law, policy, and outdated technologies, serve to hinder the exchange of information. Privacy laws, prohibitions against data mining by law enforcement and defense agencies, and restrictions concerning the role of the military in investigating and policing U.S. citizens often serve to discourage interagency collaboration and the development of tools to facilitate such collaboration. New policies, regulations and training programs will be necessary to ensure that new technologies are leveraged to the fullest extent possible and to maximize information sharing while still respecting individual privacy and civil liberties.

To the extent that information *is* presently being shared, and collaborative decision making and shared situational awareness *do* occur, these activities are achieved largely by ad hoc, non-automated, inefficient and error-prone means such as voice communications, email, point-to-point message exchange services, and manual searching of individual databases. Often, information sharing occurs only after a security incident is already underway. Due to a lack of data standards, protocols, and shared reference models across government agencies, it can be difficult to understand how the data of other organizations should be interpreted and used. Thus, many innovative information sharing technologies already available in the private sector - such as cloud computing, data mash-ups, social media, and the use of web portals to enable data sharing by disparate users based upon credentials and permissions assigned to each - are not being adopted in the government sector.

Individually, agencies have begun to address the need for improved information sharing with policies and implementation plans regarding *intra*-agency data exchange. However, as recognized in the many documents addressing this issue, the separate efforts of the various and diverse stakeholders within the NAS must align to create an air transportation system in which information is secure but accessible to anyone authorized to receive it, whether or not such recipients are members of the organization providing the information. Today, though, because the data and network standards being used by service providers are generally not readily available, interoperability is difficult to achieve without creating customized, point-to-point interfaces. For this reason, Action Item 103 of the NSAS Air Domain Security Integration and Intelligence Supporting Plan, among other documents, directs the development of "standards and protocols and joint enterprise architecture (plus a supporting common lexicon of terms and reference data models for the air domain)…"

DRAFT

In addition to the constraints presented by the lack of standards, protocols and joint enterprise architecture is the fact that inter-organizational sharing is sometimes inhibited by culture and policy that makes agencies focus inward. For example, strict interpretation of anti-deficiency legislation in Title 31 of the United States Code precludes building systems that take into consideration the mission-related requirements of external agencies. Laws such as the Posse Comitatus Act prohibit active participation by the military in law enforcement activities, raising questions about what type of information can be shared between DoD components and law enforcement agencies. Moreover, Title 40 of the United States Codes, which governs the acquisition of information technology by federal agencies, provides very little guidance on such matters as accountability for inter-agency IT acquisitions. These ambiguities and complexities in the law introduce barriers over and above the technological ones that must be broken down before wide-spread information among government agencies can be fully realized.

Overcoming these cultural and policy hurdles will be an important part of the NextGen effort. Some progress is already being made toward this goal through the formation of COIs that are tasked with identifying authoritative data sources, producing shared reference models, service descriptions, and other metadata; and helping to foster collaboration among partner agencies, industry, and the flying public. Within the NextGen stakeholder community, a weather-related COI, and an Integrated Surveillance COI have already been organized. NextGen COIs representing Safety and Special Use Airspace are expected to be organized in the near future. However, there is not yet an effective interagency governance model to provide much needed oversight and support for these efforts.

2.3 Description of Current Operations

Commercial interests within the NAS, driven by economic necessity, have long taken a pro-active approach to communications among themselves and with their customers, and have a relatively long history of innovation in the area of information sharing in net-centric environments. Passenger carriers, for example, make flight schedules, fares, seat availability, and other air travel-related information available to their customers through the internet, both on their own websites, and by pushing information to global distribution systems such as Sabre, Travelport, and Amadeus. These systems serve as a single point of access for the airlines themselves, and for online travel planning services, allowing the latter to provide air travel passengers with a variety of tools for quick and easy retrieval of information about flights, fares, and other air travel-related matters using search tools that federate queries and let users specify multiple constraints such as destination, date, time, price, seat preference, etc.

Many airports have also begun to innovate and reorganize in an effort to facilitate better dissemination of information among their numerous constituencies. Dynamic signage indicating the availability of parking; infrastructure services to support 511 Traveler Information Services (511 Services), web access, email notification and alerts; and passenger self-tagging and bag drop services are just a few of the innovations that are being implemented at some of the nation's airports. Appendix A 1 provides additional information about current airport operations.

DRAFT

The FAA's Collaborative Decision Making (CDM) program offers another example of successful collaboration in the NAS. The CDM program develops technologies and procedures to improve information exchange and data sharing among the FAA and NAS users. CDMNet, for example, facilitates real-time, communications between Airline Operational Control (AOC) centers, Air Traffic Control System Command Center (ATCSCC) and Volpe National Transportation Systems Center that have enabled more accurate predictions of airport activity. The Department of Defense (DoD) has instituted a policy that encourages development of net-centric, service-oriented enterprise architectures to improve data transparency across the DoD, and the individual Services have responded with implementation plans of their own. Similarly, the FAA's System Wide Information Management (SWIM) program seeks to support the goals of NextGen by encouraging development of an infrastructure that will facilitate information sharing within the NAS. The Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN) is a web-based platform able to facilitate information sharing and collaboration between Federal, State, local, tribal, private sector, and international partners, enabling a real-time, interactive connectivity between states and major urban areas and the DHS National Operations Center (NOC).

Some interagency efforts are also already underway. For instance, the National Oceanic and Atmospheric Administration (NOAA) and the FAA are working with the National Center for Atmospheric Research (NCAR) and the Massachusetts Institute of Technology's Lincoln Lab on the NextGen Network Enabled Weather (NNEW) program, which will integrate meteorological data synthesized from tens of thousands of data sources, providing its users with a single, authoritative source of weather observation and forecasting data.

But, while these efforts are commendable, and are already contributing to improved situational awareness for NAS stakeholders, they are not enough. Safe, secure and optimally efficient management of the NAS demands a more highly-coordinated system for exchanging and processing large amounts of disparate information among all NAS users and stakeholders, from Federal, State, tribal, local and foreign governments, to meteorologists, to general aviation pilots. Implementations such as global distribution systems for air passenger reservations and CDMNet have greatly improved the ability of many NAS users to exchange information, resulting in increased safety and efficiency of air traffic within the NAS and an environment in which commercial airlines have been able to offer increasingly more flights. The higher volume of air traffic, however, results in heavier workloads for the air traffic controllers, flight deck personnel, security personnel, baggage handlers, ground crews, law enforcement and defense operators, and others charged with keeping the NAS working and ensuring the safety of NAS users.

As described in the Phase 2 Aviation Safety Information Analysis and Sharing (ASIAS) Concept of Operations[1], most aviation safety information collection and analysis is currently conducted with little collaboration between JPDO partner departments and agencies. The various agencies with aviation operations or regulatory roles have disparate policies, rules, standards, taxonomies, architectures and systems to analyze safety information, assess findings and create corrective

[1] JPDO Paper 08-008, September 08, 2008

DRAFT

actions. Few agency safety programs are based on safety management systems (SMS). Most tend to conduct analysis focused on known causes and incidents only within their area of primary responsibility. Further, there is often very little interaction on safety issues within agencies, such as groups in the FAA and among defense services.

Many of the systems that are used today were not designed to receive or disseminate information across a wide and diverse network, and the lack of ready access to information hinders the development of effective tools for processing it. Today's systems are tightly coupled with data sources and were not designed to support inter-organizational exposure of information in reusable services that reflect the dynamic nature of data in a constantly changing airspace. The bulk of the information between aircraft and ground terminals, or among independent organizations, is by voice communications sent over analog circuits. Many exchanges of information suffer from misunderstanding, slow data transfer rates and the need to repeat information, sometimes multiple times, before it is understood. This not only creates costly delays in decision making, but it also results in poor quality forensic records and thereby inhibits organizational learning.

Lacking suitable tools for managing information in the NAS today, many users find that information overload is a significant problem. In high-density airspace, the number of aircraft tracks appearing on the watch screens of FAA, DHS, and DoD operators, for example, is already daunting and, without the aid of additional automation, it will be difficult to accommodate either an increase in traditional air traffic or the anticipated prevalence of Unmanned Air Systems (UAS). Air traffic controllers must be able to maintain safe separation among aircraft, while law enforcement and defense operators must be able to quickly spot anomalous and/or suspicious behavior among the multitude of tracks on their watch screens, and determine an appropriate response.

As air traffic density increases, UAS usage increases, and new types of potential airborne threats are developed, more and more sophisticated tools will be needed to maintain the safety and security of legitimate NAS users and to detect and assess unidentified and anomalous objects. Unexpected behavior on the part of a particular aircraft may be explained by difficulties it is experiencing with onboard systems, or it may be evidence of hostile or criminal intent. To quickly and accurately assess an anomalous situation, operators must be able to acquire up-to-date, reliable information about flight crews, passengers, cargo, associations, criminal history, and much more, in a timely and efficient manner. Appendix A 2 provides additional information about the current state of Security and Law Enforcement operations in the NAS and Appendix A 3 discusses National Defense operations in more detail.

Effective management of the tremendous volume of air traffic within the NAS demands that operators have ready access to information that goes well beyond just the location of the aircraft. Information about delayed flights, flights being held for connections, changes in airport configurations, airport protocols, or security procedures, must all be taken into account by flight crews, ANSPs, and security, law enforcement and defense personnel. Finding all of the information that is relevant to the situation at hand can mean sifting through vast amounts of

DRAFT

data, much of which may not even be relevant. In today's NAS, operators have few tools at their disposal to ensure that they receive the information they need, while eliminating the information they do not need. Appendix A 1 provides additional information about operations in the area of Civil Aviation.

The inability to automatically ingest and process information effectively presents barriers to growth, poses safety and security issues for both civil aviation and military operations in the NAS, and hinders industry's ability to exploit new business opportunities in the air travel and air cargo arenas. Safe expansion of air traffic volume is constrained and law enforcement, security and national defense missions are compromised by a lack of adequate tools for processing and analyzing the vast amounts of information required to make decisions that could have life-or-death implications. Detailed accounts of the current situation concerning information exchange for Civil Aviation, Law Enforcement and Security Operations, and National Defense are provided in Appendix A.

2.4 Modes of Operation for the Current Situation

The NAS is a system of systems that, at the highest level, can be thought of as four component systems-- Airspace, Airports, Aircraft, and Ground-based Operations Centers -- each of which is itself a complex system of systems. Each component system, and in turn, each of the component systems within these components, must operate both as a cohesive, independent whole, with data and information exchanges occurring among internal nodes, and also as a component within the larger system of systems, where communications must occur across multiple systems. Modes of operation for each system, and each component, can include

- Nominal Mode –systems are functioning as intended and operations are proceeding normally
- Degraded Mode – the system is functioning sub-optimally
- Maintenance Mode – one or more systems, or system components, is undergoing maintenance
    - Routine Preventive Maintenance – one or more physical components is undergoing preventive maintenance
    - Remedial Maintenance – one or more physical component is undergoing repair services
    - Upgrade Service – one or more physical components is being upgraded

In a system as complex as the NAS, an individual system, such as an aircraft, or a system component, such as an onboard transponder, may operate in a degraded mode, without causing degradation of the entire NAS. On the other hand, extraneous events can result in significant and wide-spread operational degradation. Inclement weather, for example, can force all four of the high-level NAS component systems to operate in degraded mode for a particular geographic region. Acts of terrorism can result in degraded operations across the entire NAS, as was the case on September 11, 2001.

DRAFT

Cyber security modes can vary enormously from one system to the next. Currently, the underlying information exchange and infrastructure services within the NAS are relatively independent, with very little formal integration among the information exchange systems created by the various NAS constituencies. While the National Institute of Standards and Technology (NIST) recognizes five cyber security modes of operation, and despite the multiple levels of classification of information that changes hands within the NAS.

Key management is critical for encryption and user credentials. However, there is currently no coordinated or comprehensive guidance, certification authority, or registration authority for encryption of data across the entire NAS, nor is there a comprehensive analysis of all of the NAS systems and the inter-dependencies among them that may affect NAS modes of operations.

2.5 User Classes and Organizations

The organizations and individuals that use the NAS and/or participate in NAS-related exchanges of information, constitute a diverse and wide-ranging set, including federal, state, and local government agencies and their subdivisions, commercial organizations, labor unions, and the individuals, such as air travelers, pilots, and security personnel, who use the NAS either in a personal capacity, or in the context of their roles within an organization. There is currently no comprehensive catalog of all of the NAS users.

2.6 Development and Support Environment

Within the Federal government, with the exception of programs that are specifically created as joint, interagency efforts, much of the planning for technology acquisitions and new system development is carried out by the individual agencies – or even the separate components of individual agencies - with relatively little regard for interagency or even *intra*-agency requirements. Although efforts are underway by all Federal NextGen partners to improve information exchange capabilities, most information systems currently in use were designed and developed in isolation from the systems of external organizations, and support environments are maintained independently as well.

When the operational processes of one organization require access to information maintained by another organization, such access has traditionally been achieved by developing specialized, point-to-point interfaces that allow information to pass between the two organizations' information management systems. When access to new or additional information resources is required, yet another point-to-point system must be created. Similarly, if other organizations acquire a need for the same information, specialized point-to-point interfaces must be developed for those systems as well. The current environment is one in which the exchange of information is inefficient and costly, and the practical effect is to discourage agencies from engaging in information sharing.

DRAFT

Information exchange across and within agencies is further hindered because there is no shared space within which architects and systems engineers can collaborate – virtually, or otherwise – on cross-agency, enterprise-wide architecture, standards development, systems design, or application development. This lack of easy access to data resources serves not only to make system-to-system communications costly in terms of both labor and acquisitions, but it also hinders innovation.

Finally, although there are numerous directives requiring that agencies share information, there are few interagency oversight mechanisms to ensure that new acquisitions and development projects are undertaken in a way that will further the objectives of such directives. There are no mechanisms for monitoring, measuring, or reporting on what information is being shared, or should be shared, nor are IT departments required to implement or maintain their systems in a manner that benefits external users.

DRAFT

3 Justification for and Nature of Changes

3.1 Justification for Changes

Although it is the safest and most efficient airspace in the history of aviation, the NAS has nearly reached the limits of its capacity to serve its stakeholder communities. In 2003, Congress recognized that the nation needs to leverage the unrealized potential capacity of the NAS in terms of profitability, efficiency and effectiveness, and it enacted Vision 100-Century of Aviation, directing that the FAA lead a collaborative effort with other key federal agencies to effect the changes necessary to do so. The implementation of Net-Centric Operations is a key element of the NAS modernization.

In order for the NAS to act as a business enabler rather than a chokepoint, air traffic routing must be efficient and flexible; safety and security regulations must support, not hinder, the ability of industry to expand and innovate. The current system's inability to respond to new needs or to harness new technological opportunities significantly limits the ability of the NAS to encourage economic growth. From the Colonial Post Road system to the Eisenhower Interstate Highway, transportation infrastructure has been a major enabler of economic growth in this country. To create an environment in which the NAS continues to be a force multiplier for the nation's business, all NAS users must have easy and timely access to appropriate, authoritative sources of information, to ensure that everyone is operating with the same accurate and up-to-date information about the conditions in the NAS.

The enhanced, shared situational awareness afforded by such access will enable high-quality, collaborative decision-making among the various government and non-government participants, ensuring that:

- government agencies charged with the responsibility of ensuring NAS safety and security have interagency shared situational awareness to effectively manage air traffic, monitor the airspace, maintain airport security, ensure the safety and security of all users, and preserve the relatively unrestricted use of the NAS that individual air travelers, businesses, and general aviation (GA) owners and operators have enjoyed to date;
- industry and government have shared situational awareness to respond effectively to the needs of their customers and market forces; to improve the quality of the NAS experience for air travelers and cargo shippers; and to ensure that communities and the environment are not endangered by the activities taking place within the NAS; and
- individual NAS users such as commercial flight crew members, airline executives, GA pilots, and government personnel, have shared situational awareness to conduct their activities in a safe, secure, and healthy environment.

DRAFT

The quality and reliability of data used for planning and decision making are impacted by the way information is gathered, stored, and shared. Current data and information management practices jeopardize data integrity and introduce barriers to the effective sharing of information among NAS stakeholders. Data is frequently moved across business or operational units by developing hard-coded, point-to-point interfaces that are usable only by the specific recipient system for which the information was originally intended. When another business or operational unit requires the information, a new interface must be developed. This is not only time-consuming, but is costly as well. Overuse of data warehouses, a dearth of information about data provenance, and difficulties in accessing authoritative data sources has created an environment in which data that may not be up-to-date, reliable, or authoritative is often disseminated from systems that are many transactions removed from the system which originally produced the data.

The challenges to information sharing created by current data and information management practices make it difficult for stakeholders to respond effectively to the ever evolving information exchange requirements that emerge in a rapidly changing NAS. NAS users cannot currently realize the shared situational awareness necessary to effectively monitor trends, identify and eliminate safety and security risks, and minimize deviations from regulations to keep the NAS running safely and efficiently, and to implement improvements to NAS operations.

In the face of increased NAS usage, shorter time frames for decision making will be required if safety and security are to be maintained. The present need to reconcile differing or poorly understood data, and lack of consistent, up-to-date, reliable, and authoritative data by all participants in the decision-making process impedes effective communications and delays decisions. Fostering a culture in which information sharing occurs as a matter of course, except where business, privacy, or security restrictions prohibit it, IX Services that readily facilitate communications within and across agencies and industry are needed. Implementing such services will require accurate, robust, and complete definitions of the data, data resources, and existing data service throughout the NAS, and must be driven by thorough analyses of data exchange requirements.

Machine-readable meta-data are needed to enable human users and systems to properly interpret the data they are receiving, to filter out superfluous data, to perform data analysis, and to present data in user interfaces that support high quality, timely decision-making. For example, a much denser and more precisely managed NAS will require computational comparisons set to alert aircrews and controllers about where and when weather-related problems can be expected to occur. But identifying the impact of weather using evolving forecasts requires precise and well-defined calculations of the planned location of an aircraft over the course of its flight compared to the forecasted and/or detected locations of convective weather, lightning, wind shear, icing conditions, etc. While identifying those coincident locations by sight alone has been adequate in the current NAS, processes such as this must be modernized and automated if the NAS is to expand beyond current capacity.

DRAFT

In 2008, aviation contributed nearly 5% of the U.S. Gross Domestic Product.[2] If the NAS is to continue as an economic force, it must be able to support new business opportunities, a sizeable portion of which will be devoted to aviation-related information technology. Information resources, including data sources and established information exchange services, must, therefore, be discoverable, not only by end-users but by software developers, to encourage development of new applications for using those resources. To create an environment in which businesses can innovate and grow, information resources must be registered in searchable data and metadata registries that are accessible to any authorized NAS information user.

The future NAS operating environment, as described in the NextGen ConOps, requires a transformed approach to information sharing and management in order to realize needed capabilities and benefits at an affordable cost while improving safety; protecting security of the passengers, cargo and the nation; and reducing the overall environmental impact. This can only be accomplished through the implementation of Net-centric Operations as a campaign of business process transformations that leverage the technological advances.

3.2 Description of Desired Changes

The essence of net-centricity is the exchange of information in a trusted, secure manner to improve or transform operations. A net-centric NAS means a NAS network populated with all available data (planning, operations, and post operations; raw and processed) needed to keep all of the many NAS systems operating as a cohesive whole, and to provide decision makers with the information they need to make well-informed business, mission, and operational decisions. Information in a net-centric environment is readily available to the right users at the right place at the right time. In a net-centric environment, users at any level can get what they need and contribute what they know.

To accomplish this, significant changes, both technological and cultural, will be required. Not only must systems within NextGen be networked and interoperable, but operations must become inherently collaborative. The organizational mindset concerning how data is obtained, used, and shared must change as well. Government and commercial entities must change the way they exchange information, and this will entail a significant change in cultural norms and governance environments.

Specifically, the following changes must occur:

Policy and governance

- A NAS information exchange governance entity must be established to create an information exchange infrastructure, data and policy standards, and performance metrics to track the quality of situational awareness established and maintained by net-centric information exchange activities, and to measure opportunity costs of shortfalls in such activities;

[2] *Federal Aviation Administration: An Historical Perspective, 1903-2008*

DRAFT

- The Office of Management and Budget (OMB) must hold Federal agencies accountable for compliance with NextGen standards, with non-compliance resulting in appropriate budgetary reductions;
- "Vision 100" Congressional guidance must be fully implemented by recognizing the JPDO as the interagency entity empowered to interact directly with NextGen constituents regarding all elements of NextGen implementation;
- Procedures and policy guidance to facilitate NAS partner agencies in quickly establishing memoranda of understanding, interconnect agreements, and computer matching agreements must be developed.

Acquisition

- An interagency, coordinated architecting and funding process is necessary to cultivate an information-centric, services-based approach to information exchange activities, rather than an approach that emphasizes systems acquisition;

Technical Implementation

- NAS-level common services must be implemented to include information security, privacy, information assurance, common messaging and metadata tagging, and identify management;
- An inter-agency testing and experimentation environment must be stood up, to facilitate proof-of-concept initiatives, prototype development of information services, demonstrations of new capabilities, and testing;
- Procedures for coordinating interagency enterprise architecture development, cross-agency certification and accreditation procedures, and change and configuration management;

Process and methodology

- The JPDO must develop an enduring business process analysis and information exchange facilitation capability for all constituents of the NAS, including a standardized methodology for data vocabulary development, metadata tagging and other data and services standardization activities designed to make data and services discoverable and reusable across the entire NextGen stakeholder community;
- The JPDO must provide support for COIs for de-conflicting data vocabulary development and for facilitating other COI activities.

Elements of this new, net-centric environment, for the most part, should be transparent to the operators and users of the NAS. Operations must continue as usual or improve, with net-centricity serving as an operational element that is behind the scenes in the realm of information exchange. Information exchanges must be effortless for the users, but must occur according to a clearly-defined, well-governed set of processes that ensure their timeliness, accuracy and precision.

3.2.1 Drivers

The aggressive goals of NextGen – to include accommodating a significant increase in airspace density, radically decreasing ecological footprints, increasing aviation security,

DRAFT

maintaining current levels of safety in an increasingly high-volume NAS, and improving the commercial aviation business case – drive the need for improvements that can only occur with the implementation of efficient and secure exchange of information within the NAS. The following factors drive the sense of urgency in realizing the NextGen Net-Centric Operations vision:

- The high cost of labor that would result from supporting increased traffic density and tempo in the absence of a network-centric information exchange environment;
- The need for immediate improvements to aviation security;
- The need to manage information overload by (1) enabling machine-to-machine data exchanges (e.g., data exchanges that occur without human intervention or interpretation); (2) automating processes for discovering, sorting, organizing and disseminating all and only the information that is relevant to the data recipient; (3) developing user-friendly systems based on Human Factors Engineering practices;
- The inability of existing information architectures to provide the requisite infrastructure capacity, latency, and management to support high speed transfers of possibly large amounts of data from authoritative data sources to any authorized user;
- The current lack of tools to enable collaborative decision making by geographically dispersed decision makers;
- The importance of ensuring that decision-making processes are adequately informed by all relevant information, regardless of which organization's databases it resides in;
- The need to leverage national and global resources such as the smart power grid, multi-modal transportation planning and development programs, and initiatives within tangentially-related industries such as entertainment, agriculture, and manufacturing to create a NAS that is fully integrated with the world-wide community;
- The unacceptably low passenger satisfaction rates currently reported in terms of on-time arrival, safety, and dependability of the scheduled flight services;
- The difficulty in today's environment in creating integrated, forensic records of NAS activities for post-event analyses to improve safety and provide a basis for organizational learning;
- The need to minimize environmental constraints to aviation through improving the use of accurate environmental information in mission and operational decision-making; and
- The need to keep customer costs from exploding.
- The need to secure and defend the airspace over the CONUS and approaches thereto.

3.2.2 Infrastructure

NextGen requires a robust and agile infrastructure upon which the entire system will rely. The services provided across the enterprise are:

- **Information Sharing Services** - Enabling agencies, business and operational units, COIs, services, and applications throughout the NAS to collaborate in a seamless information infrastructure with Air Navigation Service; airport and flight operations;

DRAFT

shared situational awareness; compliance and regulation oversight; and security, safety, environmental, and performance management services;

- **Ground Services** - Providing surveillance, communications, and flight data management to any service provider regardless of its physical location, thus removing geography as a limiting factor for air assets and ground control;
- **Air-Ground Network Services** – Abandoning frequency-to-airspace sector mapping in favor of a dynamic network environment. Data communications are central to Trajectory Based Operations, including the use of Four-Dimensional Trajectories (4DTs) (pushback and taxi inclusive) for planning and execution on the surface, automated trajectory analysis and separation assurance, and aircraft separation assurance;
- **ANSP Infrastructure Services** - Providing "virtual tower" capabilities, with which ANSP facilities can be optimally located without being constrained by airspace proximity;
- **Aircraft Data Communications Link** - Allowing aircraft and ground assets to connect to a common, secure data network for collaborative purposes;
- **Infrastructure Management Services** - Insuring quality of service (QoS), including high-level security and reliable, authoritative data;
- **Mission Support Services** - Providing information assurance, protocols, and standards applicable for the Net-centric Infrastructure Services (access, connectivity, processing, posting, and pulling).

NextGen will provide common Information Services across the Net-centric Infrastructure. This is a central principle of the NextGen transformation – that is, the provision of a set of data and information services (a "service-oriented environment") from which each NAS participant seeking to execute flight operations can draw capabilities, whether to use with their own application or with another application.

In addition to the Net-centric Infrastructure, the provision of common Information Services across the NextGen infrastructure will create shared situational awareness among all NAS users. Initial information exchange service areas include;

- Weather Information Services
- Robust Precision Navigation Services
- Surveillance Services (Cooperative and Non-Cooperative)
- Flight Plan Filing and Flight Data Management Services
- Flow Strategy and Trajectory Impact Analysis Services
- Aeronautical Information Services (AIS)
- Geographical Information System Services (GIS)
- Environmental Information Services.

3.3 Priorities among Changes

DRAFT

In order to identify necessary changes and assign resources to accomplish them, the JPDO NCOD must lead the development of a comprehensive NAS Information Exchange Management Plan (NIEMP). The plan will not impede the efforts NAS constituents currently have underway to improve information exchange within their respective enterprises, but will give them direction for resource assignment and commitment that allows for participation in a NAS-wide sharing of information. The NIEMP will constitute a plan for implementing the changes identified in this ConOps, with priority on the following:

- Ensuring that ongoing information exchange activities within respective constituent enterprises is accommodated, if possible;
- Testing proposed changes under realistic conditions, to include policy and governance methods, as well as technologies;
- Supporting near-term, foundational elements, such as common services, exchange standards and infrastructure; and
- Facilitating implementation of other priorities, as stated in the NextGen ConOps and IWP.

3.4 Changes Considered but not Included

Throughout the earliest stages of NextGen implementation, more necessary changes will be identified. Changes considered but not included are:

- Allowing fully-independent constituent development of information exchange standards and methods – because it would not attain the vision of NextGen;
- Requiring NAS users to adopt a single-source metadata tagging and information exchange methodology – because such a methodology would be too costly to implement.

3.5 Assumptions and Constraints

The information exchange environment contemplated by NextGen is one of the largest and most complex ever attempted. Implementing it will not be painless. However, with assertive, collaborative leadership it can be accomplished. Assumptions made related to the development process include:

- The SPC will make funding decisions that support NextGen participation by their constituents;
- The SPC will ensure the participation of aviation stakeholder senior leaders; and
- NextGen partner agencies will continue in their commitment to providing resources for the joint planning and development of NextGen, as delineated in the

DRAFT

June 9, 2008 Memorandum of Understanding,[3] and will act on the recommendations of the SPC.

- NAS constituents will actively participate in COIs, Integrated Process Teams (IPT), JPDO Working Groups and other entities formed to accomplish the activities - such as process engineering/reengineering, data vocabulary and reference model development, and identification of authoritative data sources – necessary to support the exchange of information within and across government agencies.
- Partner agencies will collaborate with the JPDO NCOD in the NextGen ATS Interagency Testbed (IATB) to develop prototype services, conduct testing, and refine methods for developing, discovering, accessing and using interoperable IX Services.

DRAFT

[3] *Memorandum of Understanding Among the Department of Transportation, the Department of Commerce, Department of Defense, Department of Homeland Security and National Aeronautics and Space Administration for the Next Generation Air Transportation System Joint Planning and Development*, June 9, 2008, http://www.jpdo.gov/library/NextGenJPDOMOU.pdf

4 Concepts for the Proposed System

4.1 Background, Objectives, and Scope

The expected increase in air traffic over the coming years will require new approaches to acquiring, fusing, displaying, and interpreting information. Intelligence reports, weather forecasts, flight plans, sensor data, and other information from a multitude of sources must be discoverable and accessible to those that need it. New tools for searching, analyzing, and correlating disparate pieces of information to provide the most complete and up-to-date picture of the safety and security risks, and threats to the NAS must be developed. Such tools require access to data. Agencies must work together to create a net-centric environment within which information can be quickly and widely disseminated.

Data consumers must be confident that the information they are receiving is coming from authoritative sources. Data providers must be sure that the information they disseminate will not be misappropriated. Data sources and web applications for publishing, aggregating, analyzing, and presenting data must be easily discoverable, along with appropriate metadata to provide software engineers with the adequate information about the meaning and intended use of the data. Information in the NAS must be up-to-date and reliable, and the applications that process and present the information must be certified and trustworthy.

This section provides a description of the NextGen concept of future operations in a Net-centric NAS, examining the ways in which information will be exchanged in such an environment in the Civil Aviation, Law Enforcement and Security, and National Defense mission areas. The scenarios that are appended to this ConOps provide additional details about the information exchange requirements of the NAS, today and in the future. While this ConOps discusses some of the specific operational improvements that will be enabled by the creation of a net-centric environment, it should also be noted that one of the principal benefits of net-centricity will be the opportunities for discovering new information, and developing new, unanticipated applications that use information, that will pave the way for as yet unforeseen improvements to NAS.

4.2 Operational Policies and Constraints

The exchange of information across every level of government and among government and the public and private sectors will almost certainly entail policy and legal challenges. Law enforcement and security operators within the NAS will have access to more information, increasing the opportunities for discovering and preventing terrorism and criminal behavior. However, with increased availability of information comes an increased risk that information will be misused. The exchange of information provides new opportunities for collaborative decision making and shared situational awareness, but these opportunities cannot come at the expense of civil liberties or individual privacy, nor can they violate laws and policies such as those that restrict the use of the military for domestic law enforcement. Realizing net-centricity

DRAFT

in the NAS will require guidance from governing bodies on how agencies, whose missions, roles, and authority may vary widely, can fully leverage new information sharing technologies without infringing on civil rights.

New technology can also bring new demands for procedural oversight. Training programs to certify NAS users in the use of new technologies and procedures enabled by these technologies will be necessary, and certification programs for new applications that aggregate and process data will be needed in some cases to ensure that the information such applications disseminate is reliable and authoritative; that it is appropriate classified; and that the algorithms and procedures that process the data are adequately tested and evaluated.

System security will present significant challenges for NextGen's net-centric environment. Because information within the NAS ranges in classification level from public to Top Secret, the NextGen system, like the NAS today, will be comprised of a host of separate networks of varying levels of security – e.g., the World Wide Web, the DoD's Non-classified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET), and the Joint Worldwide Intelligence Communications, to name a few. Unlike today's NAS, however, in the NextGen environment these networks will be interconnected, enabling secure exchange of information between networks, and enabling authorized users to access information from different networks from a single workstation.

To accommodate such access, new mechanisms for authenticating users at each transaction access point will be necessary to ensure that information is secure and that only authorized users are able to access information. Safeguards will be needed to ensure that classified information is protected and accessible only to those with appropriate clearances. The security controls of the various Communities of Interest within the NextGen community must be certified and accredited by an appropriate governing organization. Policies and procedures will be needed to ensure that the security of classified information is not compromised.

A comprehensive framework to reduce the risk of cyber-terrorism and other threats to NAS cyber-security will also be essential. A recent Cyberspace Policy Review conducted by the White House concluded that a public-private partnership, with significant investment and leadership from the federal government, and cooperation with other nations, would be necessary to develop the technical standards, and national and international policy and legal norms "critical to establishing a secure and thriving digital infrastructure."[4]

Optimizing airspace usage to accommodate the expected increase in air traffic may require that airspace currently reserved exclusively for special uses such as military operations, space flight and re-entry, and flight training will be increasingly available for multiple purposes on an as-needed basis. Managing such multi-use airspace will require agreements among the diverse user groups and new guidelines for coordinating operations among multiple user groups with multiple and varying purposes. For example, the increasingly common presence of Unmanned Aerial

[4] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

DRAFT

Systems (UASs) in the NAS, including military UAS operating outside of DoD-managed, restricted airspace, will present additional challenges for safety, policy, and airspace management.[5]

Data management and data governance will present significant but surmountable challenges to the implementation of a net-centric NAS. Ensuring that data is accessible, understandable, authoritative and reliable requires well-managed, networked ontologies, or semantic models, that can be used to map data elements between heterogeneous information resources; support metadata tagging and content management; and disambiguate search terms. Best practices for developing and maintaining ontologies dictate the involvement of both data producers and data consumers in Communities of Interest (COIs) that can provide the subject matter expertise needed to develop data vocabularies and semantic data models, map vocabularies and data elements, help determine the authority of data sources, and determine appropriate roles and permissions associated with data sources. A COI governance structure to oversee COI activities is imperative to ensure that ontologies and data vocabularies adhere to standards; that they are registered in a NextGen metadata repository; and that conflicts over vocabulary terms, meaning, usage, and reliability of data, etc. are resolved quickly and appropriately.

This ConOps makes the following assumptions regarding operational principles and policies:

- The Joint Planning and Development Office (JPDO) will facilitate and oversee COI activities to ensure that ontologies and web services adhere to standards, and are discoverable and reusable;
- The JPDO will monitor information exchange-related activities and report them to the JPDO Board and Senior Policy Committee (SPC) quarterly;
- The JPDO will develop an interagency test and evaluation program to support development, integration and deployment of NextGen NCO;
- System users (human and machine) will identify themselves to the system using their parent organization's authentication mechanism, which will be calibrated in advance to reflect the level of confidence agreed upon by pre-established, inter-organizational agreement.

4.3 Description of Proposed Activities and Operations

4.3.1 Overview

In the NextGen net-centric environment, information from certified, authoritative sources will be accessible to any authorized consumer. Ontologies - formal, logic-based descriptions of the information in a given system - will serve as mediating data models to facilitate data transformation across the many NextGen systems, supporting interoperability of otherwise

[5] For example, under a 2007 Memorandum of Agreement between the DoD and the FAA, the FAA granted increased access for DoD Unmanned Air Systems (UAS) in the NAS, outside of DoD-managed Restricted Areas or Warning Areas.

DRAFT

disparate information systems. Ontologies and data vocabularies will provide guidance to application developers and application users about the precise meaning of the data available in the NextGen system of systems. Ontologies will enable metadata tagging of the NextGen information resources and services, and will make information and services easily discoverable and reusable.

Ready access to information, along with consistent documentation about the meaning and the appropriate use of the information will encourage innovation in the development of new applications for using data. Today, sophisticated technologies already exist for conducting analyses, computing outcomes, and visualizing data. Geographical information systems, for instance, merge mapping software with tools that can analyze and display data overlaid on maps, satellite images, and other visualization devices. To take full advantage of such technologies, however, access to data is essential. As more data sources become available, more and more innovative applications become possible.

4.3.2 Civil Aviation

The operational improvements envisioned for the NextGen ATS depend on the implementation of a net-centric environment in which information can flow freely between disparate systems. Anticipated improvements in trajectory management, for example, contemplate automation services to enable flight crews and Air Navigation Service Providers (ANSPs) "to collaboratively and continuously assess (monitor and evaluate) constraints (e.g., airport, airspace, hazardous weather, sector workload, Navigational Aid (NAVAID) outages, security) and associated Traffic Management Initiative (TMI) mitigation strategies" and to "dynamically adjust both pre-departure and airborne trajectories in response to anticipated and real-time constraints."[6]

The ready accessibility of data in the NextGen net-centric environment will enable developers to build applications and/or web services that let both ANSPs and flight crews, and any other authorized data consumer, aggregate data from numerous sources and present it in user-friendly displays with interactive visualization tools. For example, flight crews might download flight plans into an on-board Flight Management System (FMS), request information relevant to their planned 4D trajectory – e.g., specific weather information published by the service known as the "4-D Weather Cube"; TFR information from federal, state, and local government agencies; and the locations of critical infrastructure, and the security volumetric expressions surrounding them - and display the information using tools that overlay it on a map of the proposed flight trajectory.

Such applications can be installed on or accessed from computers in control towers, on flight decks, or at any other location, and the information that feeds them can likewise be downloaded from any location, allowing flight crews and ANSPs to carry out flight planning in real-time,

[6] NextGen Integrated Work Plan, Appendix I, Operational Improvements. See, for instance, OI-0305 and OI-0306, p. 17.

DRAFT

based on up-to-the-minute information. In the net-centric environment, continuous, real-time data feeds keep flight crews and ANSPs apprised of current conditions, and any segment of the proposed trajectory can be viewed and evaluated against this up-to-the-minute information. For instance, should weather conditions change suddenly, requiring a last minute change in the flight trajectory, alternative routes can be proposed, visualized, and evaluated on the spot.

New applications for aggregating, fusing, sorting, and displaying surveillance data from all sources, including primary and secondary radar, and on-board transmitters such as ADS-B, will provide flight crews, air traffic controllers, and DHS and DoD operators alike with a more comprehensive view of airborne objects within the NAS, supporting a wide range a improvements to air traffic management that increase capacity without sacrificing safety.

Net-centric information sharing in the NextGen environment will, for example, support increased air traffic within the NAS by providing access to aggregated surveillance data that will enable automated, time-based metering of aircraft to optimize air traffic flows and improve efficiency in the use of runways and airspace in high density environments (OI 0325). Aircraft equipped with the appropriate avionics will be able to view aggregated air traffic information on onboard displays to augment visual separation on approaches in low-visibility situations. (OI 0316) The improved air traffic situational awareness provided by applications that aggregate and display surveillance data in onboard systems will support aircraft self-guided merging and spacing onto a single runway (OI 0326), further expanding the capacity of the NAS to handle increased air traffic volume.

Controller-Pilot Data Link Communications (CPDLC) will give air traffic controllers and flight crews the capability to exchange information in the form of digital messages. In information exchange situations that currently can be effected only through voice communications, the added capability of augmenting such messages with digital exchanges through CPDLC will reduce the risk of miscommunication that is common in voice-only exchanges, and will enable communications in some situations where today even voice communications are impossible.

Both commercial airlines and GA pilots will enjoy greater flexibility as a result of the increased capacity for air traffic afforded by a net-centric NAS. Real-time accessibility of data concerning restricted, special use airspace will allow pilots to effectively navigate around such airspace when it is in use, and will facilitate dynamic airspace management, allowing otherwise restricted airspace to be used for GA activities when it is not being used for special operations. Data-capture and dissemination capabilities enabled by net-centric services will create opportunities for airlines to optimize their operations, as well. For instance, net-centric information exchange services can support access to real-time, automated or semi-automated dissemination of Pilot Reports, providing first-hand information about runway conditions or obstructions or safety hazards (e.g. low-level winds) observed by onboard sensor devices. Commercial air passengers will have improved access to information about flight schedules, delays, airport security policies and procedures, onboard services, and a host of information that today is difficult to assemble.

DRAFT

In addition to the increased capacity for air traffic within the NAS, access to data concerning air traffic, airspace usage, user-defined displays of weather conditions, TFR, airport information, maintenance records, personnel data, passenger information, etc. will enable and encourage the development of innovative new analytic tools that combine seemingly unrelated data sets to derive new and otherwise undiscoverable information that may lead the way to improvements in automated route planning, scheduling, security, and other applications. The ability of DHS agents, for instance, to routinely conduct flight risk profiles will be greatly improved in the net-centric environment of NextGen, as decision-making tools that can automate some of the flight risk assessment processes become more feasible. Applications that automatically aggregate and analyze flight plans; conduct criminal background checks using federated query capabilities; incorporate and process information about weather, the location of critical infrastructure, intelligence alerts, etc. and use algorithms and other heuristics to assign a risk level to every flight – something that is currently not possible - will be possible in the future net-centric environment.

It is expected that the presence of UAS will increase substantially in the NextGen environment, including non-military UAS, which may be used for such activities as transporting goods, conducting scientific research, pipeline reconnaissance, forest-fire monitoring, and more. The net-centric environment of NextGen will be crucial for enabling the communications between UAS avionics and Ground Control Stations (GCS) and/or UAS crews, and between ATC and GCS.

4.3.3 Security and Law Enforcement

The inaccessibility of information has played a central role in allowing hostile actors to carry out terrorist and criminal acts within the NAS. According to the 9-11 Report, for example,

> Because the FBI had not been informed in January 2000 about [9-11 hijacker] Mihdhar's possession of a U.S. visa, it had not then started looking for him in the United States. Because it did not know of the links between Khallad and Mihdhar, it did not start looking for him in January 2001.[60] This incident is an example of how day-to-day gaps in information sharing can emerge even when there is mutual goodwill. [7]

In the NextGen net-centric environment, information will be published and available to authorized subscribers as a matter of course, making information sharing less ad hoc and helping to close gaps in information sharing.

Consider, for example, the near tragedy that occurred on December 25, 2009. Umar Farouk Abdulmutallab, an airline passenger traveling to the United States from Nigeria via Amsterdam, evaded security and managed to board a Detroit-bound flight carrying a quantity of highly explosive material and a chemical detonator. Abdulmutallab's name was in the Terrorist

[7] http://govinfo.library.unt.edu/911/report/911Report_Ch8.pdf

DRAFT

Identities Datamart Environment (TIDE) database at the National Counterterrorism Center; KLM Airlines records indicated that he paid cash in the amount of nearly $3000 for his plane ticket – a security red flag; State Department records showed he had a valid U.S. visa; chatter heard within the intelligence community indicated that Al Qaeda was planning a suicide attack to be carried out by a Nigerian.

While no single, isolated piece of information related to Abdulmutallab was sufficient to raise an alarm, the aggregation of information, had it been presented to security agents in a single report, might have been sufficient to do so, possibly resulting in his being placed on a no-fly list before he ever got a chance to board an airplane. In the NextGen net-centric environment, authorized security agents and law enforcement officers will be able to subscribe to regular data feeds from federal databases such as TIDE, State Department visa application databases, airline ticket sales databases, and intelligence community reports. Ready accessibility to such data resources, together with metadata and shared information models for performing data transformations, will enable developers to create federated and/or faceted search services, semantic document analysis services, topic-based document classification tools, and other innovative applications to provide the improved, shared situational awareness needed to maintain security in the NextGen ATS.

Improved surveillance data, resulting from combining and reconciling data feeds from all FAA, DHS, and DoD surveillance sensors and transponder feeds from cooperative aircraft will increase the capacity of security and law enforcement operators to detect and intercept unauthorized aircraft entering the NAS, and to interrupt and prevent the commission of crimes in the NAS. Net-centricity will make it possible to aggregate and correlate such information as flight plans, aircraft registration, and pilot and flight crew identification and histories, with enhanced sensor data, allowing security operators to more easily view and sort the aircraft in a given area. Programmable heuristics can be used to look for characteristics that may indicate malicious or criminal intent, automatically flagging such tracks for additional scrutiny by security and law enforcement agents. Programs that correlate surveillance data, flight risk levels, and security volumetric expressions around critical infrastructure can automatically monitor flights to ensure that they do not encroach on airspace in which they are not authorized to fly. The wide-range of information from multiple sources to which NextGen automated alert systems will have access will allow for alerts to be issued according to sophisticated rules, while avoiding the problem of over-alerting that has dampened enthusiasm for automated alert systems heretofore.

Flights of interest can be collaboratively tracked and assessed by Federal, state, and local agencies using NextGen's net-centric information sharing capabilities, enhancing the ability to quickly and decisively determine the nature of the threat and the appropriate response. Collaborative track monitoring will, moreover, provide those tasked with coordinating and carrying out interdictions with an enhanced picture of both the threat's location and status, and the location and status of responding Blue Forces, and other friendly aircraft. Such improvements will not only increase the time that decision makers have to assess, plan for and respond to threats, but will provide them with far more information for doing so than has previously been possible.

DRAFT

4.3.4 National Defense

In the NextGen environment, surveillance source, track, and geographic data will be distributed over an enterprise network and used by DoD Command and Control (C2) facilities providing air traffic management, security, defense, and other services. C2 systems will be capable of publishing and subscribing to specific track and geographic air domain information, as well as pre-flight information such as flight plans and intelligence reports. Net-centric sharing of data and information will provide significant advantages for national defense. In the event an anomaly or threat is detected in-flight, pre-flight information will be immediately accessible by ATO Security, AMOC, NORAD, and other security partners in a common operating picture, to facilitate their efforts to identify, locate, assess, and respond to the anomaly or threat. Integration and correlation of surveillance sensor data, common track identification, and interagency sharing of information from all sources will provide security partners with an enhanced common operating picture and improved shared situational awareness. Automated flight anomaly alerts will be disseminated to appropriate recipients if sensor data indicate that a flight has deviated from its flight plan or is otherwise engaged in anomalous behavior that meets pre-established criteria for involvement of DoD components such as NORAD/NORTHCOM. The ability to share surveillance data across agencies will enable air domain security partners to quickly and confidently confirm that a surveillance track-of-interest identified by a DEO at AMOC, for example, is the same track that appears on the watch screen of an air defense operator at NORAD.

Agreements between Canada and the US and between Mexico and the US for sharing, through net-centric information sharing systems, surveillance sensor data, track histories, flight plans, and aircraft and crew profiles will be an important component in US efforts to protect the NAS. In the event that an unauthorized approach from outside the NAS is attempted, shared surveillance track data from Canada and Mexico will provide US security and defense partners with the information they need to locate, identify, track and respond to the aircraft. Increased surveillance information sharing with other foreign partner nations will expand the scope of shared domain awareness for more global visibility and enable increased warning of and response time to an incursion or impending incursion.

Should interdiction be necessary, NextGen integration of cooperative and non-cooperative surveillance information, including data from Nav Canada and from the Mexican Directorate General of Civil Aviation (DGAC), will provide operators with a more complete picture to inform decision makers and direct actions. With ready access to any available pre-flight information, NextGen's net-centric information sharing services will provide interagency security partners with data that can be used to anticipate intent, resulting in an increased probability of a successful outcome.

Increasingly, DoD is relying on access to airspace outside of DoD-managed Restricted Areas for domestic operations, exercises, training, and testing involving UASs. In the NextGen net-centric environment, automated real-time scheduling, trajectory planning, and the ability to update and disseminate TFR and SUA information to flight crews, air traffic controllers, military pilots and

DRAFT

UAS operators will ensure that these operations can be carried out safely and expeditiously, and without harm or inconvenience to the public or other NAS users.

4.4 Modes of Operation for the NextGen ATS

The NextGen Air Transportation System, like the current NAS, will be a complex system comprised of Airspace, Airports, Aircraft and Ground-based Operations Centers and systems. NextGen is expected to operate in all of the modes of operation delineated in Section 2.4. However, it will be necessary to conduct a comprehensive analysis of the possible degradation modes in NextGen. To date, no such analysis has been conducted. Such an analysis should should, among other things, include an in depth study of the dependencies among systems and agencies. What, for example, are the possible implications for commercial air travel in the event an emergency, law enforcement, or national security operation is underway? What are the implications to other systems if one or more systems is operating in degraded mode? These matters must be thoroughly studied and understood so that NextGen partner agencies can be adequately prepared for all contingencies.

4.5 User Classes and Other Involved Personnel

While NAS user classes in the NextGen era may remain largely the same as they are in the current state, the NextGen era will see NAS users less as segregated members of independent communities, and more as equal members of the larger NextGen community. In the NextGen era, there will also be an explicit recognition that the traditionally acknowledged user classes subsume not just NAS end-users –i.e., air travelers, commercial airline pilots and flight crews, GA pilots, baggage handlers, ground crews, TSA security personnel, CEOs, intelligence analysts, ANSPs, Air Traffic Controllers, Defense Sector Operators, AMOC Detection Enforcement Officers, etc. - but system engineers, architects and developers as well. Appendix B constitutes an initial accounting of some of the user classes today and in the NextGen era, and begins to catalogue the information exchange requirements that exist today and the current- and future-state technology and policy issues that affect these requirements.

Two factors will be critical in establishing identity in the NAS: the quality of the credentials and the provenance of the credentials. In some cases, a user may establish personal identity using a credit card, but this is considered much less authoritative than a US Passport or credentials issued by a Federal employer under Homeland Security Presidential Directive 12 (HSPD 12).

4.6 Development and Support Environment

In the NextGen environment, an interagency, coordinated architecting and coordinated funding process will help ensure that new system designs and IT acquisitions will conform to net-centric data and service standards, and will deliver the information exchange requirements demanded by NextGen. The suite of documents that comprise the NextGen vision for Net-centric Operations, including the NextGen Information Exchange Architecture, the NextGen NCO Strategic Plan

DRAFT

and Roadmap, a set of NextGen Information Exchange Services Requirements, and this NCO ConOps, will provide direction for system architects, engineers and developers in every sector.

NCO Infrastructure Services will provide a collaborative development environment in which engineers can discover existing data resources and application services, metadata describing those resources and services, and tools for developing and linking new data sources and services to the NextGen environment. Both operators and engineers will participate in COIs tasked with identifying and designating authoritative data sources and NextGen information assets, developing information reference models and data vocabularies, developing and documenting roles and permissions associated with data sources, and coordinating with the NextGen Information Exchange governance body to ensure that newly networked data, metadata, and services comply with cyber security, privacy, and other information-related policies, regulations and laws. Automated monitoring and reporting systems will ensure that any service interruption is minimal. In the case of flight critical systems, automated switchover to redundant services will be included in the system design.

Operational environments are maintained independently by individual agencies. This is expected to continue in the NextGen era. However, the wholly integrated, interdependent nature of NextGen dictates that agencies will be subject to far more external dependencies than ever before. But there is currently little clarity concerning specific agency responsibilities in connection with systems that support either joint operations or the independent operations of multiple agencies. Agencies will need clearly articulated agreements about planning and funding; change management; performance measures; maintenance, etc. with respect to such shared systems.

NextGen partner agencies, having different operational requirements, may have different certification procedures for one and the same service. Weather service requirements, for example, may be different for air traffic controllers than they are for Detection Enforcement Officers at AMOC. Certification of a service by the FAA does not imply that the service is appropriate for all possible consumers. Service consumers will need access to accurate information about the status of a given service with respect to particular agencies and particular operational requirements. Furthermore, it is not obvious who will bear the responsibility for developing certain key, shared capabilities such as federated search over metadata and service registries.

Within this integrated, interdependent NextGen environment, clear guidelines outlining agency responsibilities must be established and a governance authority must be appointed to ensure compliance.

DRAFT

5 Operational Scenarios

Scenarios and use cases provide the foundation for such architecture products as concepts of operations, node connectivity charts, operational sequence diagrams, and information exchange matrices. For net-centric operations, these products are essential to describing the user experience, identifying information exchange requirements, and describing the role of information exchange services in enabling NextGen stakeholders to conduct operations in the NAS. Many of the scenarios used in this ConOps were developed for other NextGen topic areas by other working groups and COIs. In some cases, these scenarios have been annotated with additional information about the specific net-centric, informational aspects of the operations that the scenarios illustrate. Other scenarios will be developed specifically to illustrate net-centric operations in NextGen. Appendix C lists the scenarios that have been or will be developed in support of this NCO ConOps, and indicates the topic area from which the scenario originates.

Scenario development is an on-going process. Over time, this ConOps will incorporate a growing set of scenarios that represent many detailed applications and uses of NextGen net-centric operations, from the perspective of all stakeholders, including end-users and engineers.

DRAFT

6 Summary of Impacts

Virtually every business process in the NextGen system will be significantly affected by the introduction of Net-centric Operations. Most importantly, net-centricity will increase scalability, adaptability, and flexibility of NextGen information systems, thereby supporting three critically important changes to the NextGen operational environment:

- shared situational awareness among agencies, organizations, and individuals;
- a climate of collaborative decision making; and
- the use of automation to process, analyze, present and disseminate information.

These three changes will revolutionize operations and offer organizations the opportunity to optimize their workforces and business processes, from both the operational, end-user's perspective, and from the engineering/technical development perspective.

6.1 Operational Impacts

Operator participation is crucial to realizing improvements from the introduction of net-centricity. Operators accomplish the missions, and net-centric technologies and methods assist the operators. Developers cannot identify information exchange requirements – operators command that domain. While dramatic operational improvements are credited to net-centricity, it is operator input that allows the improvement to happen.

Major operational impacts for this Net-centric ConOps include:

- Increased operator involvement in activities traditionally carried out only by developers, such as information exchange requirements development;
- A greater commitment of Operations and Maintenance resources to services and information exchange infrastructure efforts;
- Increased flexibility in the integration of new methods and technologies into operational environments;
- Radically altered operations at the outset, which drive the rapid evolution of operations as NextGen participants develop an understanding of the new environment and start to leverage it in ways not previously imagined;
- A shared situational awareness among geographically dispersed operators to ensure all participants in an event are making decisions using the same reliable, up-to-date, authoritative data;
- Efficient and collaborative decision making environment in which all decision makers can access any information to which they are authorized relevant to an unfolding event;
- An environment that permits deeper and more timely discussions of options and consequences, and provides a means of quickly bringing late joiners up to date;

DRAFT

- Detailed forensic records of collaboration activities and the information exchanged therein, permitting better post-event analysis by management, safety analysts, legal authorities, and other interested stakeholders;
- Improved team training opportunities, and continuous process improvement of systems and procedures;
- Automation of processes that are currently time consuming and labor-intensive;
- Increased availability of innovative applications and tools for processing, analyzing and displaying data.

6.1.1 Flow Management

NextGen emphasizes the collaborative and/or automated decision-making process between Airline or Flight Operations Centers (AOCs/FOCs), the flight deck/cockpit, and ground control components of the Air Traffic Management system. To the maximum extent possible, decisions in NextGen will be made at the local level, with an awareness of system-wide implications. This implies an increased level of decision-making authority by flight crews and their operations teams at AOCs. Traffic information, available to ground-based and onboard displays, will allow pilots to collaborate with ground control operators on the best strategy for their preferred trajectory based on real-time contingencies. Information exchanges between these type of users and ANSPs in the NextGen enterprise may require proprietary data protection. In some cases, where the users are special government operators, the information exchanges may require classified information protection to secure the data.

6.1.2 Weather

Weather can be a high-impact, disruptive influence on the efficient flow of air traffic through the NAS. However, the increased availability of aviation-specific weather information to all NextGen stakeholders can reduce the potentially detrimental effects of weather on safety, fuel economy, system throughput, and environmental impacts by providing opportunities to integrate weather information with decision-making tools for strategic and real-time tactical planning. A single authoritative weather information source will provide improved awareness of weather-related hazards for operators, and will afford opportunities for systems engineers and developers to create improved interfaces for displaying appropriately contextualized weather information on the flight deck, in the control towers, and at security and national defense operations centers alike. The aviation weather service will draw data from traditional weather reporting systems, and aircraft and other sensors found en route, including those on UASs specifically deployed for weather collection. Other weather-related data sources include commercial weather services, airborne automation systems, human users, and the National Oceanic and Atmospheric Administration.

6.1.3 Aviation Security

NextGen emphasizes unified command and collaborative operations among ANSP, defense, law enforcement and security providers, as well as commercial and private sector NAS users such as commercial airlines, general aviation owners and operators, labor unions, cargo shippers and air

DRAFT

travelers. Each user class is associated with specific roles, responsibilities, and information access restrictions. Net-centric information services will, for example, abide by privacy laws, ensure that personally-identifiable information is protected, and secure potentially sensitive or even classified information, by ensuring that access rights are robustly managed.

6.1.4 Environmental Management

The enhanced capability to assess, avoid, and/or mitigate the environmental impacts of aviation-related activities is a key improvement in the NextGen Environmental Management System (EMS) approach. The availability of digital information exchange services will support improved collection, analysis, and exchange of information needed to assess environmental issues, and plan and implement environmental goals and effective solutions at operations and mission levels, reducing environmental impacts and constraints. For example, environmental considerations can be identified and factored into trajectory-based operational planning and integrated into ATM automation systems to inform real-time decision making. Further analysis and exchange of environmental information can be performed to ensure unnecessary environmental impacts are avoided where possible and environmental constraints to capacity are reduced. Aircraft characteristics coupled with atmospheric conditions that promote the production of environmental impact can be identified and factored into the original plans and modifications of TBO. More efficient routing of aircraft is expected to improve air quality through reduced emissions, and allow excessively noisy aircraft to avoid noise sensitive areas. Further analysis of information affecting environmental impacts can be performed as necessary to assess fines or provide incentives. Other impacts will be identified as this business area continues to evolve.

6.2 Organizational Impacts

Implementing a Service Oriented Architecture (SOA) for managing and exchanging data and information is only partly a technology challenge. Equally or perhaps more challenging are the cultural and organizational changes that will be required. Participation in interagency information exchange development activities must become as important as traditional operational mission activities. Activities such as inter-organizational coordinated architecting, collaborative software development, and COI participation to identify and designate authoritative data sources and create shared reference models, data vocabularies and other metadata, must be regarded as integral and indispensable steps in the organizations' own business processes. Achieving this objective will require that organizations commit portions of their operational budgets to non-parochial, interagency development and implementation activities, and that they undertake a deliberate effort to change organizational culture to embrace these transformations.

One of the most significant organizational impacts will result from the increasingly efficient operations. Net-centric operations will provide a collaborative environment and shared situational awareness among previously isolated government IT systems. Reusable data and software applications, offered as web-based services that can be accessed by any authorized user, will enable NextGen stakeholders to make use of information and information-related services

DRAFT

far more efficiently, greatly reducing development time and costs associated with IT acquisitions and maintenance.

The workforce in the NextGen era will certainly change. For example, a significant increase in air crews will be necessary to accommodate the increase in air traffic. The day-to-day activities of air traffic controllers and supervisors are expected to change as they begin to leverage new technologies for handling data. Important changes to the workforce are expected to involve significantly better social skills in working through multi-party decisions and the ability to leverage the technology in new and creative ways without increasing the risk to passenger, aircrew or cargo safety. Training and gaining experience in using the system or in responding to new and more challenging NextGen operations will be an important aspect of evolving the skills of operators.

The locations and numbers of air control centers, air operations centers, etc. are unlikely to change during the early stages of net-centric operations in the NextGen era. The full and true capabilities offered by this system need to be fully experienced to plan for changes such as consolidations or proliferations.

6.3 Impacts During Development

The entire process of developing systems and services will undergo radical change as a result of NextGen. Instead of making a single delivery of a major system, development of the NextGen and its associated net-centric operations will be ongoing after the target goals are achieved. Users will find new ways to use the systems, operators will find new information needs and air transportation system component owners will find new ways to characterize their elements. New information services and their related systems and new presentations of the resulting data will create a continuing need for system and service delivery. Systems will mature through evolution and ongoing minor changes instead of periodic deliveries of significant changes.

Fundamentally, development will change from the current model where each agency is largely isolated from each other to a future state in which the agencies and organizations work together to share their information services with each other and with unexpected consumers. Policy and governance need to be carefully considered to avoid anti-deficiency issues among government agency budgets. New development processes which are more dynamic and leverage the existing information services need to be created and implemented. User development initiatives that make use of mash-up tools and that build on a foundation of high-quality, flexible Software-as-a-Service (SaaS) applications will emerge. This will necessitate a significant change to development processes, including

- requirements definition,
- budgeting and advocacy,
- testing internal to the service provider,

DRAFT

- creation of inter-organizational testing to verify usability by all consumers, both external and internal, anticipated and unanticipated,
- community outreach and cultural awareness programs,
- configuration management,
- security engineering to ensure authorized access is preserved.

An effective inter-organizational governance model provides for its own evolution as users gain more experience in NextGen and find better ways to work together.

During the development and deployment phases of each service, a period of transition will be required, which implies additional resources dedicated to running both systems in parallel.

DRAFT

7 Analysis of the Proposed System

7.1 Summary of Improvements

Major improvements for NextGen resulting from Net-Centric Operations advances include:

- Reduced time to make decisions
- Improvements in the quality of decisions
- More effective and efficient transfer of responsibility between operations centers
- Increasing flexibility in the integration of new methods and technologies into operational environments.

Ready access to information by any authorized user, and sophisticated technologies for aggregating, correlating, analyzing, and displaying that information are among the key capabilities that net-centricity will bring to NextGen. These capabilities will result in better situational awareness for all user groups within the NAS, and will create an environment that fosters and supports collaborative decision making, reduces the time needed to make decisions, especially in emergency situations, and improves the informational basis on which decisions are made, resulting in better and more effective decisions. For example,

- Passengers will have better access to information about
    - flight schedules;
    - weather-related delays;
    - changes to security procedures;
    - airport services;
    - onboard services, etc.

  reducing the time needed to plan trips and navigate airport security, making air travel more efficient and enjoyable.

- Flight crews and air traffic controllers will have better information about
    - weather, TFRs and other circumstances that may affect their flight plans;
    - departure and landing requirements;
    - airport gate availability;
    - the position of aircraft, security volumetric expressions, TFRs and weather systems relative to their own current position and their anticipated positions,

  improving safety of air travel, reducing the time required to do flight planning pre-flight, and enabling real-time, in-flight trajectory changes that reduce costly delays and expand NAS air traffic capacity.

- Security, law enforcement, and defense operators will have better information about
    - Background and current status of terror suspects;

DRAFT

    - Unauthorized incursions into restricted airspace;
    - Intelligence reports that affect NAS security;
    - Identity and location of track-of-interest,

  improving their ability to prevent terrorism and other criminal acts before they can be launched, and to assess and respond to threats and anomalous activity already underway.

- Software developers will have better information about
    - The availability of data resources;
    - The meaning and intended use of data elements,

  encouraging rapid development of new and innovative systems that will drive further improvements to safety, security and efficiency within the NAS.

NextGen capabilities will be enabled by the implementation of

- Networked ontologies and data vocabularies that support
    - semantic interoperability of disparate systems; and
    - metadata tagging and search of all NextGen information resources, allowing potential information consumers to discover data sources and unstructured content from multiple sources.
- Semantic Service Oriented Architecture, featuring re-usable, web-based data exposure services that enable authorized consumers to access data on a publish/subscribe basis or by special request.
- Programmable heuristics and other analytic tools that leverage the wide range of readily accessible information available in the NextGen environment.
- Federated search across multiple databases through a single point of access, allowing users to connect dispersed and otherwise isolated pieces of information and thereby discover new information.

Enhanced surveillance data will help to increase air traffic capacity within the NAS, and improve security, law enforcement and defense operations with systems that

- aggregate surveillance data from multiple sources, including primary and secondary radar and onboard avionics;
- correlate and display surveillance data with intelligence reports and other information.
- provide automated alerts to draw security agents' attention to possible hostile or criminal activities in the NAS.

7.2 Disadvantages and Limitations

The NAS in the NextGen era relies on considerable increases in information exposure to permit increased traffic density and more intensive trajectory management. The evolution of new events in the system occur much more rapidly due to the more tightly managed conditions. While this situation presents opportunities for improved

DRAFT

performance, the higher tempo operations also become dependent upon high quality information delivered in a timely manner with high dependability.

Major disadvantages of the proposed system include:

- Increased vulnerability of the NAS to cyber attacks
- Increased level of complexity in inter-organizational governance
- Increased system dependence on the availability of information.

There are other major disadvantages of the proposed system as well. Accessibility of information provides increased opportunities for misuse.

- Extensive policy and legislative reviews, possible issuance of new policies, laws, regulations, and executive orders, and creation of governance organizations will be necessary to ensure that privacy laws, civil liberties, and other legal and regulatory constraints are not violated.
- Information can be falsified and disseminated in an effort to facilitate hostile and criminal actions.
- A net-centric environment in which information is readily accessible to all authorized users may provide a platform from which hostile actors can more effectively conduct information warfare.

Diligence will be required to avert such activity.

Data can also be misinterpreted, or mishandled. It is possible for developers to create applications that use data in a manner that is inconsistent with its intended meaning, or that mishandles data in a way that results in the dissemination of incorrect information. While a net-centric environment fosters development of applications that use data in innovative and unanticipated ways, and can potentially lead to valuable technology breakthroughs, it also increases the potential for development of applications that corrupt or debase data, either intentionally or unintentionally. Oversight will be needed to guard against such occurrences.

Information sharing will require extensive agreements among federal, state, and local governments and agencies; between U.S. and foreign governments; among international and domestic partners in the commercial sector; and among government agencies and commercial sector partners. Securing such agreements may be difficult, due to issues such as lack of trust, competition, and other cultural norms that are antithetical to information sharing.

The availability of automation can create an environment in which people are overly dependent on automated systems, possibly increasing the potential for human error due to inattention or complacency.

DRAFT

Development of the high-fidelity, robust ontologies needed to support interoperability can be labor-intensive and time consuming. Skilled and experienced ontologists are in short supply and bad ontologies can be as uninformative and difficult to interpret as relational data models, thereby undermining the semantic interoperability of the net-centric system. Care must be exercised to ensure that ontologies are developed according to best practices, using accepted standards and incorporating tried and tested ontology design patterns.

7.3 Alternatives and Trade-offs Considered

The NAS today is operating at maximum capacity. The anticipated increase in air traffic over the next 15 years demands that changes be made. Improved situational awareness is a prerequisite to accommodating any significant increase in air traffic while maintaining safety and security, and better information sharing is the most effective path to improved situational awareness. Moreover, as past failures in information sharing have shown, better sharing of information among the organizations responsible for security, law enforcement and defense within the NAS is imperative to prevent terrorist attacks.

Generally, systems have been implemented to facilitate some particular business process without regard for the need to disseminate the information produced by that process to consumers outside of the organization for which the system is created. In many cases systems are isolated, even with respect to other divisions within the organization. Within the DoD for instance, Air Force, Army, and Navy systems are not interoperable across the Services. Moreover, even within the individual Services, separate divisions maintain independent and largely incompatible systems. The same is true within the present day NAS, with systems maintained by the FAA, DoD, DHS, and the commercial sector being independent and largely incompatible, not only across agencies and companies, but also among divisions within those agencies.

Rebuilding the NAS from scratch as an integrated, centrally-managed system in which all information is accessible to every component is wholly infeasible. The incompatible systems that make up the NAS today must somehow be rendered interoperable and capable of communicating with one another. Efforts at making systems interoperable have previously resulted in the implementation of customized point-to-point interfaces that are brittle, hard to extend when information needs change, costly to build, and difficult to maintain. The effect is that information sharing remains sporadic and ad hoc, and operations continue to be carried out with insufficient information. Maintaining the status quo is not an option.

It is widely accepted that Service Oriented Architecture (SOA) is an effective mechanism for achieving interoperability among stove piped systems. This is because the infrastructure required to create a SOA environment is minimal: XML message exchange using web protocols and a standardized service description language are required. The infrastructure needed to support interactions between service consumers and service providers is already in place, for the most part. Moreover, SOA systems are flexible and

DRAFT

scalable because they serve to decouple applications from the data that those applications use, making future system modifications more feasible and less time consuming.

While SOA systems are possible without semantics, it is widely acknowledged that the lack of common understanding across organizations about the meaning and usage of data elements has created significant problems for SOA systems that do not include formal semantic descriptions of data and services. Natural languages are inherently ambiguous, and when data consumers are left to guess about the meanings of data elements, there is a high likelihood that data will be misinterpreted. Semantic descriptions, expressed in a standardized, formal, logic-based language such as OWL, support functionality such as reasoning, metadata tagging, discovery services, and data mediation. For these reasons, formal semantics are considered essential to implementing NextGen net-centricity.

DRAFT

Appendix A: Description of Current Operations by Mission Area

A.1 Civil Aviation

Commercial air passenger travel and air cargo services represent key uses of the National Airspace System (NAS), with hundreds of millions of passengers and several billion pounds of freight being moved each year. The Federal Aviation Administration (FAA) holds primary responsibility for ensuring that air travel and cargo services are conducted safely and efficiently, performing nine essential air traffic services, including;

- Flight Planning
- Separation Assurance
- Advisory
- Traffic Management-Synchronization
- Traffic Management-Strategic Flow
- Emergency and Alerting
- Navigation
- Airspace Management
- Infrastructure-Information Management.

As part of its pre-flight planning operations, the FAA receives and processes tens of millions of flight plans each year through its automated flight plan filing system. Planning functions include such activities as trajectory planning and fuel usage calculations, and ideally take into account information such as controlled and special use airspace, weather conditions, runway status, air traffic volume and flow, aircraft capabilities and equipage, the location of high-value ground assets, and the security risk level of the flight, if available. This supporting information is compiled by gathering data from numerous sources. Weather forecasts, for instance, are produced from meteorological data that must be processed and analyzed by sophisticated forecasting applications. Weather data, in turn, is needed to determine appropriate departure and arrival routes, flight trajectories, and other procedures. Anticipated airspace demand must be calculated from aggregated data on flight schedules, routing constraints, and more.

The disparate pieces of information that inform pre-flight planning today are generally contained in separate, incompatible systems. There is no centralized discovery service, or single point of access to data that would enable developers to create the sort of innovative applications that would aid operators in collecting - in a single, user-defined

DRAFT

display, or operations “dashboard” - all of the separate pieces of information they need to make sound decisions. Much of the information available to flight planners and security operators must be assembled manually, with little time available for performing the computations necessary for a robust analysis. As a consequence, decisions must frequently be made without adequate information. Where information exchanges are automated, they are handled primarily by point-to-point interfaces that have been built to transfer information between two specific systems. Should the information be needed by another system, yet another interface must be created. This model is rigid, costly, difficult to extend, and unsustainable in a NAS which is expected to see a significant increase in air traffic.

Air traffic controllers must coordinate the movement of aircraft, both during take-off and landing, and in the en-route environment. At high-volume airports, aircraft take-off and land in rapid succession, and the delay of a single aircraft can cause a cascade of system disruptions and delays down the line. In the future, most commercial aircraft will be equipped with more sophisticated on-board systems that can receive, process, and display tracks from nearby aircraft, enabling some amount of self-separation. However, in the NAS today, the task of ensuring safe separation between flights rests entirely on air traffic controllers. The surveillance data feeds that are displayed on the monitors of air traffic controllers are currently unavailable to flight crews, who must rely entirely on voice communications or limited textual communications from the tower.

Although inclement weather is the primary cause for flight delays, access to current and forecast weather conditions along a planned four-dimensional flight trajectory is not provided. There is no common weather picture for flight crews and controllers, and many aircraft continue to rely on Air Traffic Control personnel, dispatchers and Air Operations Centers (AOCs) to monitor weather information and convey weather advisories. While weather information provided by datalink is becoming more common, voice communications are still the only means of receiving important updates for many general aviation (GA) aircraft and, even for commercial and high-end GA aircraft that are equipped with radar, tools for integrating flight conditions and weather information into highly-efficient and user-friendly visualization systems are essential to support more effective Air Traffic Management (ATM) decision-making in the future.

Most GA aircraft have very limited access to weather and other critical information, other than that which can be communicated to them by voice, or which can be directly observed. Inclement weather can pose significant safety issues for GA aircraft, and affordable on-board systems to provide up-to-date information, decision support, and trajectory planning are not available. Notices to Airmen (NOTAMS) and Pilot Reports (PIREPS) provide information critical to the safe conduct of GA aircraft, including weather conditions, Temporary Flight Restrictions, Altitude Reservations, and other Special Notices NOTAMS and PIREPS are accessible through the internet, but better mechanisms for discovering the relevant information among these documents is needed.

DRAFT

Cross-agency collaboration is critical for maintaining safety in the NAS. However, in the current state, when cross-agency collaboration occurs, it tends to be informal and issue-driven, rather than systematic and comprehensive. Most sharing among agencies is limited to direct human-to-human communication networks, use of web sites and forums, and some Federal groups with specific and limited missions such as the Interagency Committee for Aviation Policy (ICAP) and the DoD Policy Board on Federal Aviation. Senior agency leaders generally inform one another of aviation safety issues common to both organizations through direct contacts. FAA technical staff and military services alert colleagues at other agencies of key issues or problems through groups such as the Commercial Aviation Safety Team (CAST) and ICAP.

Formal sharing is just getting underway in certain sectors of aviation. In 2007 the FAA, NASA, and industry partners of CAST joined together to form Phase 1 ASIAS: a systematic, integrated, trusted, collaborative environment in which the commercial flight operations community could discover and resolve commercial aviation system safety issues. The ASIAS organizational structure has three basic components:

- The ASIAS Executive Board (AEB) which manages activity and coordination
- The Issue Analysis Team (IAT) which identifies shared issues, and forms Working Groups (WGs) to assess particular issues (such as wrong runway departures and collision alerts) and perform benchmarking analyses
- The Repository Integrator which manages the flow of safety information between and among the participating organizations.

The ability to easily access and disseminate information is vital in the commercial sector, as well. Passenger airlines and air cargo companies must plan routes and schedules, taking into account both predicted and actual market demand, the schedules and routes of other carriers, availability of flight crews, union contract provisions, evolving rules and regulations governing work hours, security procedures, aircraft maintenance, airport usage, and much more. As already noted, the commercial sector has created sophisticated systems for managing much of their information exchange requirements. However, better connectivity to enable more automation will be needed to meet the challenges of the future.

Airports constitute an important and complex component system within the NAS, with airport operations encompassing a wide range of services in support of passengers, airlines, GA operators and owners, security, cargo, maintenance, engineering and support, and surrounding communities. Effective and timely communications among the numerous constituencies is crucial to ensuring that

- passengers reach their destinations safely and on-time, with their baggage intact;
- airport security is not breached, and flights are not endangered;
- cargo is loaded, tracked, and delivered efficiently;
- baggage is screened and handled appropriately;
- commercial and GA aircraft alike can enjoy access to the nation’s airports; and
- environmental impacts on surrounding communities are minimized.

DRAFT

In the civil aviation environment, the lack of automation in integrating, visualizing, and processing all of the data that must be tracked, the inability to disseminate digitized information in appropriately contextualized, user-friendly displays, and the absence of common authoritative data sources increase the likelihood of miscommunication and delays. As the volume of air traffic within the NAS increases, these problems will become more and more pronounced. Current methods of exchanging information cannot support a rapidly changing environment with significantly faster operational tempos.

A.2 Security and Law Enforcement

The Department of Homeland Security (DHS) holds primary responsibility for security and law enforcement in the NAS. DHS components, including the Transportation Security Administration (TSA), Customs and Border Protection (CBP), and Immigration and Customs Enforcement work to assess, prevent, and respond to threats to the U.S. involving the air transportation system.

CBP is charged with securing the nation's borders against narcotics smuggling, human trafficking, and terrorism. At the Air and Marine Operations Center (AMOC), CBP's Air and Marine Operations Surveillance System (AMOSS) receives, fuses, and monitors air surveillance data from multiple sensor technologies, including over 400 land-based radars (long-range, terminal, and air defense) owned and operated by various agencies; Short Range Radars (SRRs), Tethered Aerostat Radar Systems (TARS), Unmanned Aerial Vehicles (UAVs), Automatic Identification System data from Navy and Coast Guard ships, Blue Force Tracker (BFT) satellite tracking devices, remote video surveillance cameras, Airborne Warning and Control System (AWACS) aircraft, and cooperative surveillance systems such as Automatic Dependent Surveillance-Broadcast (ADS-B) and Airport Surface Detection Equipment-Model X (ASDE-X).

When available, AMOSS correlates surveillance tracks on the AMOC Detection Enforcement Officer's (DEO) watch screen with flight plan data provided by the FAA, displaying the aircraft's call number, country of origin, heading, air speed, altitude, and departure and destination airports for a selected track. DEOs can acquire additional information about the aircraft, its owner(s), crew, and passengers by querying various external and internal databases, accessible through AMOSS.

In addition to its well-known airport passenger screening operations, TSA receives, assesses, and distributes intelligence information related to transportation security; develops policies, strategies, and plans for dealing with threats to transportation security; serves as the primary liaison for transportation security to the intelligence and law enforcement communities; and works with the FAA Administrator to plan and coordinate activities that may affect aviation safety or air carrier operations.

At the Freedom Center (formerly known as the Transportation Security Operations Center), there are several air traffic and surveillance systems in use, including the CBP's AMOSS, the DoD's North American Aerospace Defense Command (NORAD) Contingency Suite (NCS), the FAA's Enhanced Traffic Management System (ETMS),

DRAFT

and the TSA-FAA Automatic Detection and Processing Terminal (ADAPT) V2. The ADAPT V2 system combines the AMOSS surveillance capability and user interface and provides users with access to various internal and external databases. Information about FAA-TSA Airspace Authorizations and Waivers, State Department diplomatic clearances, stolen aircraft, European Union banned and restricted aircraft, US and Canadian aircraft registration data, and more is accessible through the ADAPT system.

Despite the innovations at AMOC and the Freedom Center, there is much room for technological improvement and increased connectivity. AMOSS and ADAPT provide a single point of access to databases which are largely incompatible with one another. Data from external systems are only accessible in AMOSS and ADAPT through point-to-point interfaces, and there is no capability for federated search or automatic correlation and analysis of information. Separate queries to each database must be submitted manually by the operator conducting the search, making search more time consuming and laborious than necessary. Currently, there is no standardized methodology for accessing and aggregating data from disparate databases. Data provenance and reliability are difficult to assess, since the origin, authority, and timeliness of data sources can be hard to trace. In many cases, data must be transformed from its source format and entered into a central database from which it can be queried by TSA and AMOC personnel. Data standards are not well documented and misinterpretation, and consequent misuse, of data remains a problem. Substantial increase in the volume of air traffic - commercial, GA and UAV - will compound these problems.

Extensive communications among the multiple partner agencies are required to cue and coordinate air security law enforcement operations. Many of these activities are handled exclusively by voice communications, with little capability for sharing information digitally. Phone-in reporting of suspicious activity serves as a central source of information for DHS. Such communications, while crucial and irreplaceable, should be supplemented by systems capable of recording and disseminating the information both for improved operational efficiency and for after-action analyses. In addition to the significant collaboration and exchange of information that security of the NAS requires among government agencies, collaboration and efficient, secure exchanges of information between agencies and the commercial and private sectors are also necessary. Airlines and airports, for example, must provide TSA with certain information about travelers and cargo, and TSA, in turn, must cross-reference the information with passenger watch-lists and other intelligence. Conversely, airports and airlines must be able to receive timely information from the government about such things as policy and procedural changes that affect their business processes.

A.3 National Defense

The Department of Defense (DoD) is responsible for detecting, tracking and conducting surveillance of aircraft operating within the NAS and in the approaches to the US and Canada in support of its air sovereignty and air defense missions. In coordination with CBP and the FAA, the US and Canada's joint NORAD and US Northern Command identify anomalous behavior and/or unauthorized utilization of the NAS, determine

DRAFT

intent, and prepare for, plan, and execute responses to threats, including, if necessary, the use of lethal force.

The DoD currently relies on FAA cooperative and non-cooperative surveillance sensors as a primary source of information about anomalous and suspicious activity in the NAS. In coordination with the FAA, the DoD operates radars and conducts air traffic safety operations in the airspace for which it is primarily responsible. Although improved since 9-11, current data feeds from DoD and FAA surveillance systems, as well as information feeds from law enforcement and other sources, are not uniformly integrated because of bandwidth limitations. Sharing information and surveillance data is done predominantly through manual information exchange processes and verbal communications.

Efforts are currently underway to improve non-cooperative surveillance coverage, and the mechanisms by which DoD and DHS integrate and correlate surveillance data. The C2 Gap Filler program is on schedule to demonstrate a prototype system that will integrate sensor data from FAA, DHS, and DoD surveillance sensors and display a common track on the watch screens of both DoD and DHS operators. This program will improve the ability of the two agencies to exchange track-of-interest information seamlessly and confidently.

In addition to conducting its air sovereignty and air defense missions, the DoD uses the NAS to conduct flight training operations. In today's NAS, permanent restrictions are enforced on airspace used for these operations. A lack of shared situational awareness, and the inability to conduct real-time trajectory planning and dynamically manage such special use airspace make it difficult to allow other NAS users to access the airspace, even when it is not being used for training operations. Such underutilization of airspace presents a barrier to fully realizing the potential capacity of the NAS, especially hindering the ability of the airline industry to exploit new business opportunities. Future NAS operations should consider ways in which airspace can be dynamically managed, being used on an as-needed basis by a broader spectrum of NAS users.

DRAFT

Appendix B: User Operations

NAS Mission Area	Operational Area	Information Type	Information Nodes (data providers and recipients)	Sector	Technology – Current State	Technology – Future State	NextGen Operational Improvements	Policy Issues	Technology Issues
Civil Aviation	Flight Planning	Proposed flight trajectory; current and forecasted weather information; flight crew information; aircraft information; TFRs; location of critical infrastructure	FAA Flight Planners	Federal Government	Web service upload; manual and automated trajectory analysis; web search; voice communications; PiReps	Automated trajectory planning tools; publish-subscribe data exchange services; 4D trajectory visualization services; 4D Weather Cube; TBO		User access to network; authentication of users; reliability and trust of automated tools; certification of weather forecasting applications, presentation services; privacy protection laws;	Identity Management Certification Authority Registration Authority Encryption Data access Data tagging Data discovery/queriability/presentation
			DHS/TSA/CBP	Federal Government					
			Flight Crew	Commercial Sector					
			AOC Dispatchers	Commercial Sector					
			GA Owners/Operators	Private and/or Commercial Sector					
			UAS Operators	Federal and/or Commercial Sectors					
	Weather Information Services	Weather sensor data; current weather conditions; weather forecasts	Weather sensors	Federal and/or Commercial Sectors	Datalink; Web service; voice communications	Meteorological data fusion services; 4D data visualization applications		Authoritative data sources; certification of information display applications	
			NOAA/NWS	Federal Government					
			FAA Flight Planners	Federal Government					
			Flight Crews	Commercial Sector					
			AOC Dispatchers	Commercial Sector					
			DHS/CBP	Federal Government					
			DoD/N-NC/AF North	Federal Government					
			UAS Operators	Federal and/or Commercial Sectors					
	Flight Risk Profiling	Proposed flight trajectory; current and forecasted weather information; flight crew information; aircraft information; passenger information; aircraft registration information; location of	Flight Crew	Commercial Sector	N/A – Flight risk profiling is not currently done.	Automated information exchange services; automated data analysis tools.		Restrictions on data-mining by law enforcement; privacy protection laws.	Encryption Privilege Management
			DHS	Federal Government					
			FAA Flight Planners	Federal Government					
			FAA Security Personnel	Federal Government					
			Intelligence Community	Federal, State and Local Governments					
			AOC Personnel	Commercial Sector					

DRAFT

NAS Mission Area	Operational Area	Information Type	Information Nodes (data providers and recipients)	Sector	Technology – Current State	Technology – Future State	NextGen Operational Improvements	Policy Issues	Technology Issues
		critical infrastructure							
	Baggage Handling	Destination information; passenger data; baggage weight and size data	Air Travelers	Private Sector				Privacy Personally Identifiable Information	
			Baggage Handlers	Commercial Sector					
			Flight Crew	Commercial Sector					
			Ticket Agents	Commercial Sector					
			DHS/TSA	Federal Government					
	Air Traffic Management/ Take-off and Landing	Gate availability; runway status; wind speed, direction	AOC	Commercial Sector	Voice communications	4D Weather Cube; brake sensors; automated reporting avionics; net-centric publish-subscribe services;			Data communications Voice communications
			Air Traffic Controllers	Federal Government					
			Flight Crews	Commercial Sector					
			Ground Crews	Commercial Sector					
			Airport Maintenance Crews	Commercial Sector					
	Airport Operations/ Passenger Check-in	Passenger identification; flight information; baggage information; passenger special needs; airport security policies; flight status;	Air Travelers	Private Sector	Online check-in; airport-based kiosks; passenger identification cards (driver's license, passport); arrival/departure information display monitors; 511 services			Privacy Personally Identifiable Information	User Authentication
			Ticket Agents	Commercial Sector					
			Baggage Handlers	Commercial Sector					
			DHS/TSA	Federal Government					
	Airport Operations/ Passenger Boarding	Boarding pass; flight/aircraft status; estimated departure time; passenger needs; runway status; weather conditions	Passenger Controller		Boarding pass scanners; flight status monitors; voice communications				Data communications Voice communications
			Flight Crew						
			Maintenance Crew						
			Baggage Handlers						
			Ground Crews						
			Air Traffic						
	Air Traffic Management Operations/ En-route	Weather; surveillance data; flight status; aircraft status; pilot status	FAA ATC	Federal Government				Privacy protection laws	
			Flight Crew	Commercial Sector					
			AOC Personnel	Commercial Sector					
			Weather Forecasters	Commercial and Government Sectors					

DRAFT

NAS Mission Area	Operational Area	Information Type	Information Nodes (data providers and recipients)	Sector	Technology – Current State	Technology – Future State	NextGen Operational Improvements	Policy Issues	Technology Issues
			Cooperative and Non-cooperative Sensors	Federal Government					
	Aircraft Maintenance	maintenance schedule; flight history; maintenance records; maintenance personnel information							User authrentication Authoritative data sources Metadata tagging
	Aircraft Operations/ Trajectory Based				N/A				
Security and Law Enforcement	Border Protection Surveillance Monitoring/ Anomaly and Suspicious Activity Detection	Surveillance data; flight plans; weather information; aircraft call numbers; surveillance video	FAA Flight Planners Flight Crews NOAA/NWS DHS/CBP DoD/N-NC GA Owners/Operators Sensors	Federal Government Commercial Sector Federal Government Federal Government Federal Government Private and/or Commercial Sectors Federal Government	Surveillance data feeds received by AMOSS system; no correlation with other C2 systems (e.g., N-NC); manual querying of separate databases; voice communications	C2GF sensor fusion services in areas with multiple sensor coverage; automated correlation with other C2 systems; federated querying over multiple LE and intel databases; automated alerting services		Privacy protection; restrictions on information sharing with DoD entities; provenance, certification and authoritativeness of fused and correlated track data;	User authentication Encryption Key management Authoritative data sources Data tagging
	Intent Assessment	Surveillance data; intelligence reports; flight plans; weather information; aircraft registration data; flight crew identification; surveillance video; passenger manifests; cargo manifests; location of critical infrastructure, TFRs and SUAs	Sensors FAA Flight Planners Federal, State, and Local databases TSA Flight Crews AOCs	Federal Government Federal Government Federal, State, and Local governments Federal Government Commercial Sector Commercial Sector				Privacy Personally Identifiable Information	User authentication Encryption Key management Authoritative data sources Data tagging
	Interdiction Operations	Surveillance data; flight crew	Sensors		Blue Force Tracker (GPS); AMOSS	ADS-B; trajectory management tools;			

DRAFT

NAS Mission Area	Operational Area	Information Type	Information Nodes (data providers and recipients)	Sector	Technology – Current State	Technology – Future State	NextGen Operational Improvements	Policy Issues	Technology Issues
		identification; friendly force position information	Interdiction team – Pilots, Ground-based Operators Commend Center		surveillance data feeds; voice communications; hand signals	digital message exchange services			Network security
	Law Enforcement	Surveillance data; aircraft registration data; flight crew identification; crime statistics; criminal records; informant tips			Blue Force Tracker (GPS); AMOSS surveillance data feeds; voice communications; hand signals	ADS-B; trajectory management tools; digital message exchange services			Information assurance User authentication Authoritative data sources
National Defense	Surveillance Monitoring/ Anomaly and Suspicious Activity Detection	Surveillance data; intelligence reports; flight plans; weather information; location of critical infrastructure, TFRs, and SUAs							Information assurance User authentication Authoritative data sources Network security Encryption Privilege management Network latency and bandwidth
Information Exchange	Data Transfer	Structured data; unstructured text/documents;		Government, Commercial, and Private Sectors	Voice communications; email; point-to-point interfaces; XML	Metadata repository; federated search; XML; OWL; WSDL; web-services; ontology management systems		Data provenance; cyber security; privacy protection	Information assurance User authentication Authoritative data sources Network security Encryption Privilege management Network latency and bandwidth
Enterprise Architecture									Information assurance User authentication Authoritative data sources Network security Encryption Privilege management Network latency and bandwidth

DRAFT

NAS Mission Area	Operational Area	Information Type	Information Nodes (data providers and recipients)	Sector	Technology – Current State	Technology – Future State	NextGen Operational Improvements	Policy Issues	Technology Issues
Software Acquisition and Development	Web-service Development							Information assurance User authentication Authoritative data sources Network security Encryption Privilege management Network latency and bandwidth	

DRAFT

Appendix C: Scenarios

Scenario ID	Business Area	Scenario Description	Source	Primary POV	Actors	Entities	Version	Duplicate Scenario	Owner
NCO-1	Weather	Reduced Airport Ops	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-2	Surveillance	Fast Business Jet Penetration from Northern Border	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-3	Surveillance	Tracking of Lost Cargo Airliner within CONUS	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-4	Weather	Convective Weather Enroute over GOM	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-5	Weather	Domestic Airline Flight	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-6	TBO	Routine Instrument Flight Rules (IFR)	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-7	Weather	Convective Weather Forecasted before Descent into Classic Airspace	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-8	Surveillance	Lost Pilot Blunders into Controlled Airspace	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-9	Surveillance	Degraded ADS-B	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-10	Surveillance	Fast Business Jet Penetration from Gulf of Mexico	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-11	Surveillance	Off-nominal GA Flight scenario	NextGen JPE	TBD	TBD	TBD	TBD	TBD	TBD
NCO-12	TBO	Phoenix-to-Miami - Dynamic SUA	ICNS Study	TBD	TBD	TBD	TBD	TBD	TBD
NCO-13	TBO	Phoenix-to-Jackson Hole-classic airspace	ICNS Study	TBD	TBD	TBD	TBD	TBD	TBD
NCO-14	TBO	Miami to New York/JFK - flow contingency	ICNS Study	TBD	TBD	TBD	TBD	TBD	TBD
NCO-15	TBO	New York/JDK to Houston-super density airport, weather	ICNS Study	TBD	TBD	TBD	TBD	TBD	TBD
NCO-16	TBO	Phoenix to Miami -	TBO Report	TBD	TBD	TBD	TBD	TBD	TBD
NCO-17	TBO	Detroit to Washington Dulles - flow constrained	TBO Report	TBD	TBD	TBD	TBD	TBD	TBD
NCO-18	TBO	Phoenix to Bozeman - General Aviation	TBO Report	TBD	TBD	TBD	TBD	TBD	TBD
NCO-19	Safety	Safety Information Sharing among approved stakeholders	ASIAS ConOps	TBD	TBD	TBD	TBD	TBD	TBD
NCO-20	NCO	Client application developer creates a new custom application	TBD	Developer	TBD	TBD	TBD	TBD	TBD
NCO-21	NCO	NextGen Decision Maker logs in and is authorized access	TBD	Any user	TBD	TBD	TBD	TBD	TBD
NCO-22	NCO	Monitoring service detects info service fault or change	TBD	Net/Comm shift supervisor	TBD	TBD	TBD	TBD	TBD

DRAFT

Scenario ID	Business Area	Scenario Description	Source	Primary POV	Actors	Entities	Version	Duplicate Scenario	Owner
NCO-23	NCO	Info Provider determines a change to existing service is needed	TBD	Info Service owner	TBD	TBD	TBD	TBD	TBD
NCO-24	NCO	Info Provider identifies a new information service to be supplied	TBD	Info Service owner	TBD	TBD	TBD	TBD	TBD
NCO-25	TBO	Airline planner identifies routes & gates for next 6 month window	TBD	Airline Op Center	TBD	TBD	TBD	TBD	TBD
NCO-26	Airport	Routine maintenance closes a gate or ramp area	TBD	Airport Op Center	TBD	TBD	TBD	TBD	TBD
NCO-27	Airport	Shift Change among airport operations staff	TBD	Airport Op Center	TBD	TBD	TBD	TBD	TBD
NCO-28	TBO	Air crew bids on schedule	TBD	Air Crew	TBD	TBD	TBD	TBD	TBD
NCO-29	TBO	Air crew runs out of time and must be replaced due to delays	TBD	Airline Op Center	TBD	TBD	TBD	TBD	TBD
NCO-30	TBO	Aircraft is scheduled for planned maintenance	TBD	Airline Op Center	TBD	TBD	TBD	TBD	TBD
NCO-31	TBO	Aircraft experiences unplanned maintenance outage	TBD	Airline Op Center	TBD	TBD	TBD	TBD	TBD
NCO-32	TBO	Natural or man-made disaster blocks use of a region of airspace	TBD		TBD	TBD	TBD	TBD	TBD
NCO-33	TBO	UAS conducts normal border surveillance operations	TBD	AMOC Operator	TBD	TBD	TBD	TBD	TBD
NCO-34	TBO	UAS conducts normal training operations in Special Use Airspace	TBD		TBD	TBD	TBD	TBD	TBD
NCO-35	TBO	Military training operations schedules SUA	TBD	Air Force Training Scheduler	TBD	TBD	TBD	TBD	TBD
NCO-36	Safety	A flight accident occurs	TBD	Safety Analyst	TBD	TBD	TBD	TBD	TBD
NCO-37	Airport	An unplanned incident closes access to airport facilities (partial to full)	TBD	Airport Op Center	TBD	TBD	TBD	TBD	TBD

DRAFT

Scenario ID	Business Area	Scenario Description	Source	Primary POV	Actors	Entities	Version	Duplicate Scenario	Owner
NCO-38	NCO	An malicious user attacks the NCO infrastructure	TBD	NCO Service Provider	TBD	TBD	TBD	TBD	TBD
NCO-39	NCO	An unintentional incident creates NCO infrastructure outages	TBD	NCO Service Provider	TBD	TBD	TBD	TBD	TBD
NCO-40	Environment	Conduct analysis of noise compliance	TBD	Analyst	TBD	TBD	TBD	TBD	TBD
NCO-41	Environment	Conduct analysis of emissions compliance	TBD	Analyst	TBD	TBD	TBD	TBD	TBD
NCO-42	L.A. Security	Passenger flies from one domestic airport to another	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-43	L.A. Security	Terrorist seeks to fly from one domestic airport to another	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-44	L.A. Security	Passenger flies from one foreign airport to a US Airport	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-45	L.A. Security	Passenger flies from US airport to foreign airport	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-46	L.A. Security	Terrorist flies from one foreign airport to a US Airport	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-47	L.A. Security	Cargo shipper transports bulk from US airport to US airport	TBD	Customer	TBD	TBD	TBD	TBD	TBD
NCO-48	L.A. Security	Cargo shipper transports bulk from US airport to foreign airport	TBD	Customer	TBD	TBD	TBD	TBD	TBD
NCO-49	L.A. Security	Cargo shipper transports bulk from foreign airport to US airport	TBD	Customer	TBD	TBD	TBD	TBD	TBD
NCO-50	L.A. Security	Smuggler transports bulk from US airport to US airport	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-51	L.A. Security	Smuggler transports bulk from US airport to foreign airport	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-52	L.A. Security	Smuggler transports bulk from foreign airport to US airport	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-53	L.A. Security	Smuggler transports on GA/charter from US to US airport	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-54	L.A. Security	Smuggler transports on GA/charter from US airport to foreign airport	TBD	Passenger	TBD	TBD	TBD	TBD	TBD
NCO-55	L.A. Security	Smuggler transports on GA/charter from foreign airport to US airport	TBD	Passenger	TBD	TBD	TBD	TBD	TBD

DRAFT

Appendix D: Acronyms

Acronym	Definition
ADAPT	Automatic Detection and Processing Terminal
ADP	
ADS-B	Automatic Dependent Surveillance-Broadcast
AF	Air Force
AIS	Aeronautical Information Services
ALN	Aerial Layer Network
AMOC	Alternative Method of Compliance
AMOSS	Air and Marine Operations Surveillance System
ANSP	Air Navigation Service Providers
AOC	Airline Operational Control
AOS	Area of Separation or Automated Observation System
ARTC	Air Route Traffic Control
ASDE-X	Airport Surface Detection Equipment-Model X
ASIAS	Aviation Safety Information Analysis and Sharing
ATCSCC	Air Traffic Control System Command Center
AWACS	Airborne Warning and Control System
BFT	Blue Force Tracker
C2	Command and Control
CBP	Customs and Boarder Protection
CDM	Collaborative Decision Making
CDM Net	Collaborative Decision Making Network
COI	Community of Interest
CPDLC	Controller-Pilot Data Link Communications
CSPR	Center for Climate Science and Policy Research
CTA	Chicago Transit Authority
DEO	Detection Enforcement Officer
DGAC	Mexican Directorate General of Civil Aviation
DHS	Department of Homeland Security
DOD	Department of Defense
EMS	Environmental Management System
FEMA	Federal Emergency Management Agency
FMS	Flight Management System
FOC	Flight Operation Center
GA	General Aviation
GCS	Ground Control Stations
GIS	Geographical Information System Services

DRAFT

Acronym	Definition
HSIN	Homeland Security Information Network
HSPD-12	Homeland Security Presidential Directive-12
HSPD-16	Homeland Security Presidential Directive-16
IAH	George Bush Intercontinental Airport
IFR	Instrument Flight Rules
IPT	Integrated Process Teams
IWP	Integrated Work Plan
IX Services	Information Exchange Services
JPDO	Joint Planning and Development Office
LEO	Logistics and Engineering Operations
NAS	National Airspace System
NAVAID	Navigational Aid
NCAR	National Center for Atmospheric Research
NCO	Net-centric Operations
NextGen	Next Generation Air Transportation System
NIEMP	NAS Information Exchange Management Plan
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NNEW	NextGen Network Enabled Weather
NOAA	National Oceanic and Atmospheric Administration
NORAD	North American Aerospace Defense Command
NORTHCOM	United States Northern Command
NOTAMS	Notice to Airmen
NSAS	National Strategy for Aviation Security
NSPD-47	National Security Presidential Directive-47
NTSB	National Traffic Safety Board
ODP	Office of Domestic Preparedness
PIMS	Personal Identify Management System
QoS	Quality of Service
RNP	Required Navigation Performance
SFO	Supervised Flight Operations
SIPRNET	Secret Internet Protocol Router Network
SLC	Salt Lake City International Airport
SMS	Safety Management System
SOA	Service Oriented Architecture
SPC	Senior Policy Committee
SRR	Short Range Radars
SUA	Special Use Airspace

DRAFT

Acronym	Definition
TARS	Tethers Aerostat Radar Systems
TBO	Trajectory-Based Operations
TFR	Temporary Flight Restriction
TIDE	Terrorist Identities Datamart Environment
TIS-B	Traffic Information Service-Broadcast
TMI	Traffic Management Initiatives
TSA	Transportation Security Administration
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle

DRAFT

Appendix E: References

The following references were used for the development of this Concept of Operations.

1	JPDO NextGen Concept of Operations, v2.0, 13 Jun 2007
2	JPDO NextGen Enterprise Architecture, v2.0, 22 Jun 2007
3	JPDO NextGen Integrated Work Plan: A Functional Outline, v1.0, 30 Sep 2008
4	FAA NAS Enterprise Architecture 6 and NAS Toolset Version: 20090527 6.8.13
5	NASEAF Version 2.0 Volume I: Definitions and Guidelines, 30 Sep2007
6	NASEAF Version 2.0 Volume II: Product Descriptions, 30 Sep 2007
7	NASEAF Version 2.0 Volume III: Product Implementation Methodologies, 30 Sep 2007
8	FAA Air Traffic Organization (ATO) Concept of Operations for Air Domain Security, v1.0, 21 Apr 2008
9	JPDO, Network Enabled Operations (NEO) Spiral 1 Final Report, D794-10208-1, Rev A, 30 May 2008
10	JPDO, Joint NEO Spiral 1 Team, Network Enabled Operation (NEO) Spiral 1 Command Post Exercise (CPX) Report, 30 Apr 2008
11	JPDO, Integrated Surveillance Concept of Operations for the NextGen, v3.0, 16 June, 2009
12	JPDO, Paper No. 08-008, Phase 2 Aviation Safety Information Analysis and Sharing Concept of Operations, 16 Apr 2009
13	JPDO, NextGen Cyber Security Strategy, v1.0, 28 Jan 2008
14	JPDO, NextGen Weather Concept of Operations, v1.0, June 2007
15	DISA, NCES Pilot Participants Guide, v0.7, Oct 2005
16	DISA, NCES Program Overview Briefing, 30 Nov 2005
17	DOD, DOD CIO, Net-Centric Data Strategy, 9 May 2003
18	DOD, Data Sharing in a Net-Centric Department of Defense, DODD 8320.2, 2 Dec 2004
19	DOD, Net-Centric Enterprise Services War fighter Concept of Operations, v1.1D, 1 March 2005
20	DOD, The National Defense Strategy of the United States of America, March 2005
21	DOD, ASD/NII, Guidance for Implementing Net-Centric Data Sharing, DoD 8320.2G, 12 April 2006
22	DOD, DOD CIO, Net-Centric Services Strategy, Jan 2007
23	DOD, Joint Concept of Operations for the Global Information Grid (GIG) 2.0, July 2008
24	JPDO, NextGen Air Transportation System, Weather Concept of Operations, v 1.0, 13 May 2006
25	JPDO, End-State Description of the NextGen Air Transportation System, July 2004
26	FAA, Operational Evolution Partnership, Executive Overview, v 1.0, June 2007
27	JPDO, NextGen Air Transportation System, Making the NextGen Vision a Reality, 2006 Progress Report, 2006
28	US Air Force, NextGen Air Transportation System, NextGen Strategic Plan, draft, undated

DRAFT

29	MDA DS COI, Joint Implementation & Services Working Group, Services Roadmap, March 2005
30	NIEM Program Management Office, Introduction to the National Information Exchange Model, v 0.3, 12 February 2007
31	NIEM Program Management Office, National Information Exchange Model Concept of Operations, v 0.5, 9 January 2007
32	NCOIC, NCOIC Interoperability Framework (NIF), v 1.0, 16 November 2008
33	MITRE, Implementing a Net-Centric Data Access Service, Mary K. Pulvermacher, December 2007
34	IEEE, IEEE Std. 1362-1998 (R2007) - Guide for Information Technology - System Definition - Concept of Operations (ConOps) Document, 1362-1998 (R2007), December 2007

DRAFT

Appendix F: Glossary

Term	Definition
Aeronautical Information Service (AIS)	The near-real-time transmission of accurate aeronautical information, including updates on airspace restrictions; performance requirements for airspace access and operations; system outages; airport status information; static information, such as approach plates; and certain fixed airspace definitional data, such as fixed special activity airspace and airport information.
Air Carrier	The Air Carrier operational node represents the operational users of NextGen. An air carrier includes commercial passenger or cargo airlines, military air commands, business aviation, and private air vehicle operators.
Air Domain	The global airspace, including domestic, international, and foreign airspace, as well as all manned and unmanned aircraft operating in and people and cargo present in that airspace, and all aviation-related infrastructures.
Air Navigation Service Provider (ANSP)	Used generically, ANSP refers to the organization, personnel, and automation that provide separation assurance, traffic management, infrastructure management, aviation information, navigation, landing, airspace management, or aviation assistance services for airspace users.
Air Traffic Management (ATM)	The dynamic, integrated management of air traffic and airspace—safely, economically, and efficiently—through the provision of facilities and seamless services in collaboration with all parties.
Airborne Self-Separation	Refers to all aircraft within the airspace or airport movement area maintaining separation from all other aircraft within the airspace or airport movement area according to defined rules and separation criteria. The ANSP is not responsible for separation between aircraft. When authorized by the ANSP, equipped aircraft in this airspace maintain separation from all other aircraft, including those managed by the ANSP.
Airborne Separation	Refers to separation delegated to an individual aircraft to maintain separation from a designated aircraft, either in flight or on the airport movement area, such as for a crossing or passing maneuver. Separation of this aircraft from all other aircraft, including all aircraft to which separation has not been delegated, remains the responsibility of the ANSP. Pair wise separation and closely spaced parallel approaches are also in this category.

DRAFT

Term	Definition
Airborne Separation Assurance	Refers to a capability of the aircraft to maintain awareness of and separation from other aircraft, airspace, terrain, or obstacles. There are four different levels of airborne separation assurance (based on the RTCA definition)—airborne traffic situational awareness, airborne spacing, airborne separation, and airborne self-separation.
Airborne Spacing	Refers to the capability of one aircraft to achieve and maintain a defined distance in space or time from another aircraft. Separation responsibility remains with the ANSP.
Airborne Traffic Situational Awareness	Refers to flight crew knowledge of nearby traffic depicted on a cockpit traffic display without any change of separation tasks or responsibility.
Aircraft	Any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface. An aircraft can include a fixed-wing structure, rotorcraft, lighter-than-air vehicle, or a vehicle capable of leaving the atmosphere for space flight.
Airport	A defined area on land or water (including any buildings, installations, and equipment) intended to be used either wholly or in part for the arrival, departure, and surface movement of aircraft.
Airspace Classification	Airspace with a common air traffic management interest and use, based on similar characteristics of traffic density, complexity, air navigation system infrastructure requirements, aircraft capabilities, or other specified considerations wherein a common detailed plan will foster the implementation of interoperable CNS/ATM systems.
Airspace Design	The process of transforming routes, fixes, sectors, and other structural/operational elements of the NAS to ensure a safe, secure, and efficient aviation system.
Air Navigation Service Provider (ANSP)	An organization responsible for and authorized to provide air traffic management (ATM) services; communications, navigation, and surveillance (CNS) services; meteorological services for air navigation; and aeronautical information services.
Air Navigation Service Provider (ANSP) Flow Airspace	High-density, moderate complexity airspace where the flight operator executes a 4DT agreement. Trajectory Management (TM) ensures the overall flows are well behaved so that potential conflicts are kept to a minimum. Separation Management (SM) is performed automatically by ground automation. If conflicts are detected, the ground automation issues revised 4DTs to the flight operator.
Area Navigation (RNAV)	A method of navigation that permits aircraft operation on any desired flight path within the coverage of station-referenced navigation aids, the limits of the capability of self-contained aids, or a combination of these.

DRAFT

Term	Definition
Area Navigation (RNAV) Operations	Aircraft operations using an RNAV system. RNAV Operations remove the requirement for a direct link between aircraft navigation and a NAVAID, thereby allowing aircraft better NAS access and permitting flexibility of point-to-point operations. RNAV Operations include RNAV and RNP applications.
Area Navigation (RNAV) Route	An ATS route established for the use of aircraft capable of employing area navigation.
Arrival/Departure Airspace	Airspace from the top of climb or descent to the airport surface. It includes only the arrival and departure corridors in current use, but extends to en-route altitudes.
Automated NextGen Tower (ANT)	A facility where sequencing services and basic airport information are provided without the use of ANSP personnel, at a service level that is enhanced compared with typical nontowered airports.
Auto-Negotiation	The interaction among two or more systems to identify a specific operational response acceptable to the parties (e.g., flight operator and ANSP) served by the automated system. The automated systems would use the known operating constraints or user preferences to identify the preferred response.
Capacity	The maximum number of aircraft that can be accommodated in a given time period by the system or one of its components (throughput).
Capacity Management	The long-term and short-term management and assignment of NAS airspace and routes to meet expected demand. This includes assigning related NAS assets as well as coordinating longer term staffing plans for airspace assignments. It includes the allocation of airspace to airspace classifications based on demand, as well as the allocation of airspace and routes to ANSP personnel to manage workload.
Classic Airspace	Low-altitude airspace away from the busiest terminal areas (those not engaged in super-density operations) that accommodates mixed capability aircraft, including those under visual flight rules.
Collaborative Air Traffic Management	The collaborative process among the ANSP, flight operators, airport operators, and other stakeholders, to manage objectives for capacity management, flow contingency management, and trajectory management. Collaborative air traffic management (C-ATM) is the means by which flight operator objectives and constraints are balanced with overall NAS performance objectives.
Complexity	A description of how nonhomogeneous the traffic demand is. Factors that cause complexity to be higher are large numbers of vertically transitioning aircraft, large numbers of crossing paths, large variation in speeds, etc.
Community of Interest	A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information it exchanges. (*Department of Defense Directive 8320.02*, April 23, 2007)

DRAFT

Term	Definition
Conflict	Any situation involving an aircraft and a hazard in which the applicable separation minima may be compromised.
Constraint	Any limitation on the implementation of an operational improvement, or a limitation on reaching the desired level of service.
Controlled Time of Arrival	The assignment and acceptance of an entry/use time for a specific NAS resource. Examples include point-in-space metering, time to be at a runway, or taxi waypoints.
Cooperative Surveillance	The determination of an aircraft's 3D position utilizing equipment on the airframe. In comparison, noncooperative surveillance would be the determination of an aircraft's 3D position without the aircraft participating.
Demand	The number of aircraft requesting to use the ATM system in a given time period.
Enablers	Initiatives, such as (new) technologies, systems, operational procedures, and operational or socioeconomic developments, that facilitate the implementation of operational improvements or of other enablers.
Enterprise Services	Any or all of the key services that are provided to all COIs throughout NextGen, and can be characterized by the net-centric infrastructure services that provide connectivity and universal access to information; and by services that provide the collection, processing, and distribution of information. This includes Shared Situational Awareness, Security Management, Safety Management, Environmental Management, and Performance Management Services.
Environmental Management System	An organizational business process that consists of four phases. In the first "planning" phase of the NextGen EMS, the organization will identify environmental issues with the potential to constrain future capacity. These will be the focus of tactical, measurable objectives for which improvement initiatives can be undertaken during the second "implementation" phase. During the third "assessment" phase, the effectiveness of these initiatives is monitored and key performance metrics tracked. Monitoring data are then used to support planning at the organization itself in the fourth "review and adaptation" phase. In the NextGen EMS, monitoring data will also be reported at an enterprise level to support NextGen-wide planning.
Equivalent Visual Operations	The capability to provide aircraft with the critical information needed to maintain safe distances from other aircraft during nonvisual conditions, including a capability to operate at levels associated with VFR operations on the airport surface during low-visibility conditions. The ANSP personnel delegate separation responsibility to the flight operators. This capability builds on net-enabled information access, certain aspects of performance-based services, and some elements of PNT services and layered adaptive security.

DRAFT

Term	Definition
Flight Crew	The individual or group of individuals responsible for the control of an individual aircraft while it is moving on the surface or while airborne.
Flight Object	The representation of the relevant information about a particular instance of a flight. The information in a flight object includes (1) aircraft capabilities, including the level of navigation, communications, and surveillance performance (e.g., FMS capabilities); (2) aircraft flight performance parameters; (3) flight crew capabilities, including level of training received to enable special procedures; (4) 4DT profile and intent, containing the "cleared" 4DT profile plus any desired or proposed 4DTs; and (5) aircraft position information and near-term intent. Standards for the definition of a flight object are in development.
Flight Operator	The organization or person responsible for scheduling, planning, and directly operating the aircraft. Roles within the flight operator include the flight scheduler, flight planner, and flight crew and may reside with one individual or be delegated to separate individuals.
Flight Plan	Specified information relating to the intended flight of an aircraft that is filed electronically, orally, or in writing with an ANSP facility.
Flight Planning	A series of activities preformed before a flight that includes, but is not limited to, reviewing airspace and navigation restrictions, developing the route, obtaining a weather briefing, completing a navigation log, filing a flight plan, and inspecting the aircraft.
Flight Plan Filing and Flight Data Management Services	The management of data related to a flight, from the initial filing of a proposed flight to the closing of the flight plan and the archiving of the data to support performance management analyses.
Flow Contingency Management	The process that identifies potential flow problems, such as large demand capacity imbalances, congestion, a high degrees of complexity, blocked or constrained airspace, or other off-nominal conditions. It is a collaborative process between ANSP personnel and airspace users to develop flow strategies to resolve the flow problems. Examples of flow strategies include establishing routing to reduce complexity, restructuring airspace, and allocating access to airspace or runways.
Flow Corridor	A corridor is a long "tube" of airspace that encloses groups of flights flying along the same path in one direction. It is airspace procedurally separated from surrounding traffic and special use airspace, and it is reserved for aircraft in that group. There is a minimum distance that traffic within the corridor must maintain from the edge of the corridor (i.e., "the corridor walls have some thickness").
Flow Strategy and Trajectory Impact Analysis Services	This capability in NextGen provides a common "what if" function to assess potential changes in planned flights, the allocation and configuration of assets, as well as other conditions (e.g., weather, security initiatives, etc.) that may affect flight operations.

DRAFT

Term	Definition
Four-Dimensional Trajectory (4DT)	A 4DT represents the "centerline" of a path plus the positioning uncertainty, including waypoint. Positioning uncertainty includes lateral, longitudinal, and vertical positioning uncertainty. Some waypoints within a 4DT may be defined with controlled times of arrival (CTAs), which constrains the uncertainty for planning purposes. The required level of specificity of the 4DT will depend on the operating environment in which the flight will be flown. Associated with a 4DT is the separation zone around an aircraft and the aircraft intent information, which provides near-term information on the expected flight path.
General Aviation	The term used to describe any flight other than a military or scheduled airline flight, ranging from gliders and powered parachutes to large, nonscheduled cargo jet flights.
Hazards	The objects or elements from which an aircraft can be separated. These include other aircraft, terrain, weather, wake turbulence, incompatible airspace activity, and, when the aircraft is on the ground, surface vehicles and other obstructions on the apron and maneuvering area.
Human-Centric	The ATM system is designed around the capabilities and limitations of humans. It assigns functions to humans that are best performed by them, and it provides automation assistance when it can improve decision-making or make the humans' tasks easier. It does not imply that humans are always in direct control.
Human Factors Engineering	The discipline concerned with the understanding of interactions among humans and other elements of a system. It applies theory, principles, data, and other scientific methods to system design to optimize human well-being and overall system performance.
Information Services	A service that provides data and information to subscribers when and where needed in a common format. Ensures questions raised by data consumers are answered correctly and consistently.
Infrastructure Services	A service that provides communications connectivity to ensure information flows work reliably to support information communications and sharing functions.
Interconnect Agreement	An interconnect agreement is a business contract between organizations for the purpose of interconnecting their networks and exchanging telecommunications traffic. Interconnect agreements are typically complex contractual agreements, involving payment schemes and schedules, coordination of routing policies, acceptable use policies, traffic balancing requirements, technical standards, coordination of network operations, dispute resolution, etc.

DRAFT

Term	Definition
Integrated Risk Management (IRM)	A process that includes prognostic tools, models, and simulations at the strategic, operational, and tactical level to support all stakeholder decision makers and managers in the grafting of cost-effective "best practices" into the design, acquisition, deployment, and operation of aviation security system assets and infrastructures. Knowledge bases concerning threats, vulnerabilities, and practices are tailored to user profiles that proactively determine need/authorization to know.
Intelligent Agents	Within the context of this operational concept, refers to a computational system that includes the following characteristics: is aware of constraints, has goals, and operates autonomously within its construct to identify information or opportunities for human action. It is customized for an area or task, is adaptive, knows the user's preferences/interests, and can operate on their behalf (e.g., by narrowing the choices available through auto-negotiation). As such, this concept's definition is consistent with commonly accepted industry standards.
Intent	Information on planned future aircraft behavior, which can be obtained from the aircraft systems (avionics). It is associated with the commanded trajectory and takes into account aircraft performance, weather, terrain, and ATM service constraints. The aircraft intent data correspond either to aircraft trajectory data that directly relate to the future aircraft trajectory as programmed inside the avionics or the aircraft control parameters as managed by the automatic flight control system. These aircraft control parameters could either be entered by the flight operator or automatically derived by the flight management system.
Key management	Key management is the management within a cryptography system design of generation, exchange, storage, safeguarding, use, vetting, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

DRAFT

Term	Definition
Layered Adaptive Security	The security system will be constructed in "layers of defense" to detect threats early and prevent them from meeting their objective while minimally affecting efficient operations. Airports and aircraft will be designed to be more resilient to attacks or incidents. Building on the "net-enabled information access" and "performance-based services" capabilities, risk assessments will begin well before each flight so that people and goods will be appropriately screened as they move from the "airport" curb to the aircraft, or as they support aerodrome/aircraft operations. As technology matures, screening will be unobtrusive and more transparent to the individual. All people and cargo that "touch" or are carried by an aircraft will be positively identified. Responses to anomalies and incidents will be proportional to the assessed risk of the involved individuals or cargo.
Managed Airspace	An Air Navigation Service Provider provides Air Traffic Management Services; separation is delegated as appropriate to equipped aircraft.
Metroplex	A group of two or more adjacent airports whose arrival and departure operations are highly interdependent.
Near-Space Airspace	Low-density, low-complexity airspace at very high altitudes that accommodates a wide range of special operations (e.g., high-speed reconnaissance aircraft, aerostats, long-endurance orbiting unmanned aircraft systems).
Net-Centricity	For aviation transportation efforts, defines a robust, globally interconnected network environment in which information is shared in a timely and consistent manner among users, applications, and platforms.
Net-Enabled Information (NEI)	An information network that makes information available, securable, and usable in real time to distribute decision making. Information may be pushed to known users and is available to be pulled by other users, including users perhaps not previously identified as having a need for the information.
Network Enabled Operations (NEO)	The decision support and other applications using NEI for information transfer and retrieval.
NextGen Decision Oriented Tool (NDOT)	A tool that incorporates observations, forecasts, model/algorithm data, and climatology, including surface observations and weather aloft to allow full integration of weather into traffic flow decision making.
NextGen Network Enabled Weather (NNEW)	The 4D net-centric weather information network that publishes discoverable past, current, and future weather data and information for decision makers; enabling weather situational awareness when planning and executing operations across the full spectrum of the Air Transportation System.
Non-Managed Airspace	Uncontrolled, low-altitude airspace where no ANSP services are provided, except as required to coordinate entry to a different class of airspace.

DRAFT

Term	Definition
Oceanic Airspace	That airspace over the oceans of the world, considered international airspace, where oceanic separation and procedures per ICAO are applied. Responsibility for the provisions of ATC service in this airspace is delegated to various countries, based generally upon geographic proximity and the availability of the required resources.
Performance-Based Navigation	Performance-based navigation specifies RNAV system performance requirements for aircraft operating along an ATS route, on an instrument approach procedure, or in an airspace. Performance requirements are defined in terms of accuracy, integrity, continuity, availability, and functionality needed for the proposed operation in the context of a particular airspace concept. Performance requirements are identified in navigation specifications that also identify the navigation sensors and equipment that may be used to meet the performance requirement.
Performance-Based Operations	Use of performance capability definition versus an “equipment” basis to define the regulatory/procedural requirements to perform a given operation in a given airspace.
Performance-Based Services	There are multiple service levels aligned with specified user performance thresholds to provide choices to users depending on needs, required communication, navigation and surveillance performance, environmental performance criteria, security parameters, and so forth. Services will be flexible according to the situation and consolidated needs of the users. Services vary from area to area in terms of airspace and “airport” surfaces, and they vary with time as needs dictate. Preferences are established based on user capability, equipage, training, security, and other considerations. The performance-based approach is used to analyze risks (e.g., safety, security, environment) instead of “equipment-based” approaches. The performance-based services capability will enable a definition of service tiers and allow the government to move from equipment-based regulations to performance-based regulations.
Position, Navigation, Timing (PNT) Services	A service that enables the ability to accurately and precisely determine one’s current location and orientation in relation to one’s desired path and position; apply corrections to course, orientation, and speed to attain the desired position; and to obtain accurate and precise time anywhere on the globe, within user-defined timeliness parameters.
Privilege Management	A set of processes for managing the data, attributes and policies in particular that determine a user's access rights to a system. Privilege management matches data/information attributes with role-based user access privileges to determine a user's authority to access particular data.

DRAFT

Term	Definition
Required Navigation Performance	A statement of the navigation performance accuracy necessary for operation within a defined airspace. RNP Operations introduce the requirement for on-board navigational performance monitoring and alerting.
Required Navigation Performance Level or Type (RNP-X)	A value, in nautical miles (NM), from the intended horizontal position within which an aircraft would be at least 95 percent of the total flying time.
Route	A 3D path through space with no time component. Unlike corridors, aircraft can cross routes as operational need requires, with proper separation provided to all aircraft.
Safety Assurance	The independent oversight function that tests, evaluates, and certifies, as necessary, products and processes to ensure that they are safe for the public and stakeholders.
Safety Culture	The product of individual and group values, attitudes, competencies, and patterns of behaviors that determine the commitment to, and the style and proficiency of, an organization's health and safety programs.
Safety Management System (SMS)	The process that provides a systematic method for managing safety. The four components of an SMS are policy, architecture, assurance, and safety promotion.
Safety Risk Management (SRM)	The set of processes and practices by which a concept and its operation are designed and made to be safe.
Self Separation Airspace	That airspace where aircraft self-separation enables maximum user flexibility in exchange for high-capability equipage of the aircraft.
Separation Management	The function of ensuring aircraft or vehicles maintain safe separation minima from other aircraft or vehicles, protected airspace, terrain, weather, or other hazards. The function may be performed by ANSP personnel, the flight operator, and/or automation.
Separation Minima	The minimum displacements between an aircraft and a hazard that maintain the risk of collision at an acceptable level of safety.
Service Oriented Architecture (SOA)	A design for linking computational resources (principally, applications and data) on demand to achieve the desired results for service consumers (which can be end users or other services). The Organization for the Advancement of Structured Information Standards (OASIS) defines SOA as the following: A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects consistent with measurable preconditions and expectations.
Shared Situational Awareness (SSA)	The sharing of information among the processes and applications that constitute the information services function to the stakeholders in the system.

DRAFT

Term	Definition
Situational Awareness	Refers to a service provider or operator's ability to identify, process, and comprehend important information about what is happening with regard to the operation. Airborne traffic situational awareness is an aspect of overall situational awareness for the flight crew of an aircraft operating in proximity to other aircraft.
Special Activity Airspace (SAA)	A volume of airspace where certain aircraft must be restricted from transiting that airspace. SAAs may be defined for Alert Areas, Controlled Firing Areas, Military Operations Areas (MOAs), Prohibited Areas, Restricted Areas, or Warning Areas. SAAs may be available from national sources of published Special Use Airspaces (SUAs) or may be locally defined. Information associated with SAAs includes designators, the controlling agency, vertical and horizontal boundaries, separation distance, and activation schedule.
Staffed NextGen Tower (SNT)	A facility where surface and tower services are provided by ANSP personnel, providing other-than-direct visual observation, who may or may not be located at the facility.
Stakeholders	All entities that are have a vested interest in ensuring the safest and most efficient operation of the NextGen. Through performance metrics analysis and research, these entities see that the proper training is coordinated and provided to the appropriate COIs, and that other enterprise needs are met.
Super-Density Flexible Airspace	The specific airspace configurations or routes chosen in near-real time to provide flexibility and maximize arrival and departure throughput. It is smaller than or lies within super-density protected airspace.
Super-Density Protected Airspace	The charted airspace protecting super-density terminals that is somewhat larger than the actual airspace used operationally. Statically defined for low-capability aircraft that do not have access to real-time updates of airspace definition.
Surveillance Services	This service integrates cooperative and noncooperative airport surface and airspace surveillance systems, fostering real-time air and airport situational awareness and enhancing safety and security.
Trajectory Management	The function of fine-tuning trajectories as required by the airspace plan or an active flow contingency management initiative to minimize pairwise contention and ensure efficient individual trajectories within a flow.
Trajectory-Based Operations	The use of 4D trajectories as the basis for planning and executing all flight operations supported by the air navigation service provider.
Transition Airspace	Airspace that allows aircraft to transition from one classification of airspace to another while maintaining separation from other airspace and aircraft entering and exiting adjacent airspace.
Unmanned Aircraft System	A pilotless aircraft is flown without a pilot-in-command onboard and is either remotely or fully controlled from another place (ground, another aircraft, space) or programmed and fully autonomous. The UAS includes the pilotless vehicle, control system, and operator.

DRAFT

Term	Definition
Virtual Tower	A facility that provides surface and tower services without the requirement for ANSP personnel providing direct visual observation. Virtual towers may be automated or staffed.
Weather Information Services	NextGen Weather Information Service is a common service providing the following generic capabilities: sensor configuration, observation, forecast, and history.

DRAFT

Document Revision History

VERSION	DATE	DESCRIPTION
Draft Version 1.0	July 7, 2010	Post to JPDO.gov for review.

DRAFT