UNITED STATES

POSITIONING, NAVIGATION, AND TIMING

INTERFERENCE DETECTION

AND

MITIGATION PLAN SUMMARY

APRIL 2008

SUMMARY

The Department of Homeland Security (DHS) Positioning, Navigation, and Timing (PNT) Interference Detection and Mitigation (IDM) Plan was developed as the result of tasking from the United States (U. S.) Space-Based PNT Policy of December 8, 2004. The policy established responsibilities for multiple departments and agencies within the Federal government, to better plan, manage and protect PNT services, and assigned the DHS specific responsibilities governing the protection of PNT services within the critical infrastructure (CI). The IDM Plan details the DHS's initial response to the Policy implementation action and lays the foundation for further planning and actions necessary to meet the Presidential Policy responsibilities. The IDM Plan was approved by the President on August 20, 2007.

BACKGROUND AND PURPOSE

On December 8, 2004, the President signed the U.S. Space-Based PNT Policy that superseded previous Global Positioning System (GPS) policy[1] and established guidance and implementation actions for space-based PNT programs, augmentations, and activities for U.S. national and homeland security, civil, scientific, and commercial purposes. This new policy is the foundation of the responsibilities and actions necessary to achieve capability improvements and to effectively manage the GPS into the future. The policy stated that the U.S. must continue to improve and maintain the GPS, its augmentations, and back-up capabilities to meet growing national, homeland, and economic security requirements, and to meet commercial and scientific demands[2]. The formation of the DHS along with the governing Presidential Directives[3] were the result of the U.S. Government's need to prepare for, protect against, and recover from significant incidents within the U.S. that impact the critical infrastructure underpinning American society. PNT services have been widely recognized as an integral part of the technological foundation of civil and commercial worldwide infrastructure; and they have been recognized specifically as a critical component of numerous parts of the U.S. critical infrastructure. Through this recognition of the importance of PNT services, the question of system vulnerability to interference has been raised, with potential risk issues defined and quantified in completed analyses and studies. This heightened recognition is the impetus behind efforts to plan and prepare for incidents of interference to these systems, and provide guidance for the timely resolution and mitigation of interference events.

The DHS was tasked in the Policy to develop plans for: coordinating U.S. interference detection and mitigation capabilities; the collection, analysis, data storage, and dissemination of interference reports; and the development, implementation and exercise

[1] Presidential Decision Directive/National Science and Technology Council-6, March 28, 1996
[2] U.S. Space-Based Positioning, Navigation, and Timing Policy, Fact Sheet, December 15, 2004
[3] Homeland Security Presidential Directive-5, Office of the Press Secretary, The White House, February 28, 2003 and Homeland Security Presidential Directive-7, Office of the Press Secretary, The White House, December 17, 2003

of procedures to request assistance from the Secretary of Defense. To accomplish this, the plan examines current capabilities to meet the policy goals described above and determines what provisions and resources already exist within the Federal government; how they can be consolidated and improved; what deficiencies and limitations exist; the potential for process and capability improvement; and the plan for the exercise of these capabilities. The IDM Plan seeks to promote and improve cooperation and information exchange, thus enabling a prioritized response to incidents, a means of requesting assistance and the utilization of capabilities across the Federal government. Fundamentally, the plan seeks to rationalize and bring together organizations that already acknowledge current system limitations in order to better attain methodologies, practices, and solutions in the pursuit of improved National capability.

Objective

The objective of the PNT Interference Detection and Mitigation Plan is to provide a framework and guidance from which to execute responsibilities required to fulfill the directives from the U.S. Space-Based PNT Policy. The scope of the plan is to:

- Establish key responsibilities from the major stakeholders in policy implementation.
- Highlight the importance of GPS within the critical infrastructure.
- Describe the current methods of interference detection, reporting, investigation and mitigation, and ensure organizations train, test and exercise these methods.
- Improve current processes and architectures with respect to implementing policy guidance.
- Establish a baseline cooperative framework for future interference detection, reporting, investigation and mitigation capabilities.
- Provide observations and recommendations for capability improvement, plan management, and test and evaluation.
- Provide the basis for estimating President's Budget (PB) PNT funding requirements.

Methodology and Considerations

The IDM plan was undertaken as an effort to describe how organizations' current procedures and plans could be brought together to provide a more robust framework for the detection, reporting, investigation and mitigation of GPS interference. The DHS PNT Working Group, established by the plan, will address the need for new concepts of operations (CONOPS) or modifications to existing CONOPS. With the advent of future Global Navigation Satellite Systems (GNSS), it was understood that the plan is not solely written to represent GPS, but also is applicable to other space-based and ground-based PNT services, their augmentations and back-up PNT services. It is also important to note that the focus of the plan is internal to the U.S., but consideration for the future must conceptualize PNT service interference as a worldwide problem, which includes the Homeland Security elements and the protection of the U.S. critical infrastructure.

The impact of several Presidential Policies was considered and the responsibilities of key Departments examined in order to set the objectives and scope of the plan. Under these policies, the acceptance that PNT services are a component of multiple sectors of the U.S. critical infrastructure was specifically addressed.

A fundamental ideal exists throughout the plan to develop and build on current systems and capabilities in order to improve processes and provide a roadmap for future capability development. It was realized that there are multiple stakeholders, each controlling a variety of tasks and responsibilities that must be brought together to develop a cooperative framework with which to execute the plan further.

The plan analyzes and defines 'what' needs to be done, but does not attempt to determine 'how' or by 'whom'. The Volpe study on the vulnerabilities of transportation systems that rely on GPS details how disruptions to the GPS system can range from limited denial of GPS service caused by a low power, localized jammer to denial of GPS service over large geographic areas and for extended periods of time. The vulnerabilities identified in earlier studies, coupled with those identified in future vulnerability studies, will be used as the basis for assessing the impacts of interference, and defining standardized approaches to detecting, identifying, and mitigating interference. These considerations will be the scope of the DHS PNT Working Group as well as the implementation of future inter-agency agreements with regard to the execution of the concepts proposed throughout the plan, funding availability and the timeframe or schedule required for execution. The DHS PNT Working Group is a responsibility of the DHS and is composed of key DHS offices with PNT related responsibilities. For tasks that will directly impact National Space-Based PNT Executive Committee member Departments' and Agencies' responsibilities, members will be invited to participate fully in all DHS PNT Working Group activities.

KEY POLICIES, DEPARTMENTS AND AGENCIES

Under the U.S. Space-Based PNT Policy, the Departments and Agencies described below were assigned responsibilities that impact PNT services within the U.S. and the inter-departmental coordination necessary to protect PNT services in the event of interference. Applicable policy directives, along with these responsibilities, form the basis for the development and execution of this plan and the subsequent findings and recommendations necessary for successful implementation.

Policy Directives

Several Presidential Policy Directives are directly applicable to the development and further implementation of this plan. The overarching statements drawn from existing policy directives listed below provide the fundamental basis for the analysis and recommendations necessary for Federal Departments and Agencies to meet the objectives of this PNT Interference Detection and Mitigation Plan.

Homeland Security Presidential Directive (HSPD) – 5

The purpose of HSPD-5 is to enhance the ability of the United States to manage domestic incidents by establishing a single comprehensive incident management system. This policy describes the methodology to prepare for, respond to and recover from terrorist attacks, major disasters, and other emergencies, by defining a single comprehensive incident management system. Of principle importance is the foundation of a National Incident Management System (NIMS)[4] that defines a core set of concepts, principles, terminology and technologies to cover incident management.

Homeland Security Presidential Directive (HSPD) – 7

HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources[5], and to protect them from terrorist attacks. The policy is wide ranging and defines and describes the DHS responsibilities in the protection of the United States critical infrastructure. Of particular interest are the policies listed to protect the Nation's critical infrastructure and key resources against terrorist acts; which clearly define the foundation for actions and inter-departmental cooperation to be undertaken to prevent such acts. Further detail describes the extent and responsibilities of other departments, agencies, committees and offices associated with the execution of this policy. The policy also defines the responsibility for a National Plan for Critical Infrastructure and Key Resource Protection which:

- Defines strategy to identify, prioritize and coordinate the protection of critical infrastructure and key resources.
- Provides a summary of activities to define, prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources.
- Provides a summary of initiatives for sharing critical infrastructure and key resources information and threat warning data.
- Defines coordination and integration with other Federal emergency management and preparedness activities.

U.S. Space-Based PNT Policy

The U.S. Space-Based PNT Policy established guidance and implementation actions for space-based PNT programs, augmentations and activities for U.S. national and homeland security, civil, scientific and commercial purposes. The fundamental goal of the policy is to ensure that the U.S. maintains space-based PNT services, augmentation, back-up and service denial capabilities. The goals of the Policy applicable to this plan include:

- Provide uninterrupted availability of PNT services.
- Meet growing national, homeland, economic security, civil requirements, and scientific and commercial demands.

[4] National Incident Management System, U.S. Department of Homeland Security, March 1, 2004
[5] As defined in the 2006 National Infrastructure Protection Plan

To achieve these goals, the U.S. Government must:

- Maintain the GPS as a component of multiple sectors of the U.S. critical infrastructure, consistent with HSPD-7.
- Provide on a continuous, worldwide basis civil space-based PNT services free of direct user fees for civil, commercial, and scientific uses, and for homeland security through the GPS and its augmentations.
- Improve the performance of space-based PNT services, including more robust resistance to interference for, and consistent with, U.S. and allied national security purposes, homeland security, and civil, commercial and scientific users worldwide.

These goals form the basis of the responsibilities allocated to the various departments and agencies as the major stakeholders of PNT interest in the Federal government.

Cooperating and Coordinating Responsibilities

The policies described above are implemented through many other departments, agencies, State and local authorities, administrations and organizations. This plan details only those elements affecting the critical coordinating stakeholders described below; however, it is recognized that many other cooperating stakeholders may be involved in the implementation of this plan.

Department of Homeland Security

Under the U.S. Space-Based PNT Policy, the DHS was assigned the following responsibilities that are applicable to this Plan:

- Identify space-based PNT requirements for homeland security purposes to the Secretary of Transportation, and coordinate the use of PNT capabilities and backup systems for homeland security purposes by Federal, State and local governments and authorities.
- In coordination with the Secretary of Transportation, and with other Departments and Agencies, promote the use of the GPS positioning and timing standards for use by Federal agencies, and by State and local authorities responsible for public safety and emergency response.
- In coordination with the Secretary of Defense, and in cooperation with the Secretaries of Transportation and Commerce, ensure:
  - Mechanisms are in place to identify, understand and disseminate timely information regarding threats associated with the potential hostile use of space-based PNT services within the U.S.
  - Procedures are developed, implemented and routinely exercised to request assistance from the Secretary of Defense should it become necessary to deny hostile use of space-based PNT services within the United States.

- In coordination with the Secretaries of Defense, Transportation and Commerce, develop and maintain capabilities, procedures and techniques, and routinely exercise civil contingency responses to ensure continuity of operations in the event that access to the GPS is disrupted or denied.
- In coordination with the Secretaries of Transportation and Defense, and in cooperation with other Departments and Agencies, coordinate the use of existing and planned Federal capabilities to identify, locate and attribute any interference within the U.S. that adversely affects use of the GPS and its augmentations for homeland security, civil, commercial and scientific purposes.
- In coordination with the Secretaries of Transportation and Defense, and the Director of National Intelligence (DNI), and in cooperation with other Departments and Agencies:
  - Develop a central repository and database for reports of domestic and international interference to the civil services of the GPS and its augmentations for homeland security, civil, commercial and scientific purposes; and (2) notify promptly the Administrator, National Telecommunications and Information Administration (NTIA), the Chairman of the Federal Communications Commission (FCC), the Secretary of Defense, the Director of National Intelligence and other Departments and Agencies in cases of domestic or international interference with space-based PNT services to enable appropriate investigation, notification and/or enforcement action.

Department of Defense

Under the U.S. Space-Based PNT Policy, the Department of Defense (DoD) was assigned the following responsibilities that are applicable to this Plan:

- Have responsibility for the development, acquisition, operation, security and continued modernization of the GPS, while facilitating appropriate civil and homeland security Department and Agency representation and participation in these activities, and any decisions that affect civil and homeland security equities.
- Develop, acquire, operate, realistically test, evaluate and maintain navigation warfare (Navwar) capabilities and other capabilities required to:
  - Effectively utilize the GPS services in the event of adversary jamming or other interference.
  - Deny to adversaries PNT services from the GPS, its augmentations and/or any other space-based PNT systems without unduly disrupting civil, commercial and scientific uses of these services outside an area of military operations, or for homeland security purposes.
  - Identify, locate and mitigate, in coordination with Departments and Agencies, as appropriate, any interference on a global basis that adversely affects use of the Global Positioning System for military purposes.

- Ensure the earliest operational availability for modernized military and Navwar capabilities.
- Train, equip, test and exercise U.S. military forces and national security capabilities in operationally realistic conditions that include denial of GPS. In cooperation with the Secretaries of Transportation and Homeland Security, and as appropriate, with the Secretary of State, develop guidelines that facilitate these activities and Navwar training, testing, demonstrations and exercises without unduly disrupting or degrading homeland security and civil services and operations, either internationally or domestically.
- Maintain the commitment to discontinue the use of the feature known as Selective Availability designed to degrade globally the Standard Positioning Service (SPS) of the GPS.
- Facilitate access to appropriate levels of national security services and user equipment at the Federal level to meet critical requirements for emergency response and other homeland security purposes, and, on an exception basis, for civil purposes, including State or local emergency response.
- Develop improved, dedicated national security PNT capabilities, including but not limited to more diverse, flexible, and capable signals and services.

Department of Transportation

Under the U.S. Space-Based PNT Policy, the Department of Transportation (DOT) was assigned the following responsibilities that are applicable to this Plan:

- Have lead responsibility for the development of requirements for civil applications from all U.S. Government (USG) civil Departments and Agencies.
- Ensure, in cooperation with the Secretary of Defense and the Secretary of Homeland Security, the performance monitoring of U.S. civil space-based PNT services.
- In cooperation with other Departments and Agencies, promote the use of U.S. civil space-based PNT services and capabilities for transportation safety.
- Represent the civil Departments and Agencies in the development, acquisition, management and operations of the GPS.
- In coordination with the Secretary of Homeland Security, develop, acquire, operate and maintain backup PNT capabilities that can support critical transportation, homeland security, and other critical civil and commercial infrastructure applications within the U.S., in the event of a disruption of the GPS or other space-based PNT services, consistent with Homeland Security Presidential Directive-7.

Department of Commerce

Under the U.S. Space-Based PNT Policy, the Department of Commerce (DOC) was assigned the following responsibilities that are applicable to the Plan:

- Represent U.S. commercial interests with other Departments and Agencies in the requirements review of the GPS and related space-based augmentations.

- In coordination with the Secretaries of State, Defense, and Transportation and the Administrator of the National Aeronautics and Space Administration (NASA), seek to protect the RF spectrum used by GPS and its augmentations through appropriate domestic and international spectrum management and regulatory practices.

- In coordination with the Secretaries of Defense and Transportation, and the Administrator of NASA, facilitate cooperation between the United States Government and U.S. industry as appropriate to identify mutually acceptable solutions that will preserve existing and evolving uses of space-based PNT services, while allowing for the development of other technologies and services that depend on use of the RF spectrum.

- Support the Department of Homeland Security in coordinating the use of existing and planned federal capabilities to identify, locate, and attribute any interference within the United States that adversely affects use of GPS and its augmentations for homeland security, civil, commercial, and scientific purposes.

- Cooperate with the Department of Homeland Security to: (1) develop a central repository and database for reports of domestic and international interference to the civil services of GPS and its augmentations for homeland security, civil, commercial, and scientific purposes; and (2) notify promptly the Administrator, National Telecommunications and Information Administration (NTIA), the Chairman of the Federal Communications Commission (Commission), the Secretary of Defense, the Director of National Intelligence, and other Departments and Agencies in cases of domestic or international interference with space-based PNT services to enable appropriate investigation, notification, and/or enforcement action.

Director of National Intelligence

The Director of National Intelligence shall identify, monitor, and assess the development of foreign threats to the use of the GPS PNT architectures and related services; and provide information to assist the Secretary of Defense in development of countermeasures.

Other Departments, Agencies, Administrations and Organizations

Departments and Agencies detecting interference, or receiving reports of domestic or international interference adversely affecting the performance of U.S. space-based PNT services shall provide timely reports to the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence. Upon notification by the Secretary of Homeland Security:

- The Secretary of Commerce, in cooperation with other Departments and Agencies, and with the chairman of the FCC shall take appropriate and legally permissible

actions required to mitigate interference to U.S. space-based PNT services within the U.S.

- The Secretary of State shall, as appropriate, notify and/or coordinate the notification of foreign governments and international organizations in cases of interference with U.S. space-based PNT services caused by foreign government or commercial activities.

Committees and Working Groups

National Space-Based PNT Executive Committee

Under the U.S. Space-Based PNT Policy, the National Space-Based PNT Executive Committee is established and will make recommendations to its member Departments and Agencies, and will advise and coordinate strategic decisions regarding policy, architectures, requirements and resource allocations. The Executive Committee will be co-chaired by the Deputy Secretaries of the DoD and the DOT, or by their designated representatives. Its members will include representatives at the equivalent level from the Department of State (DOS), DOC and DHS, the Joint Chiefs of Staff, the National Aeronautics and Space Administration (NASA), and from other Departments and Agencies as required. Components of the Executive Office of the President, including the Office of Management and Budget, the National Security Council (NSC), the Homeland Security Council, the Office of Science and Technology Policy, and the National Economic Council, shall participate as observers to the Executive Committee. The Chairman of the FCC shall be invited to participate on the Executive Committee as a Liaison. The National Space-Based PNT Executive Committee has the following responsibilities applicable to this Plan:

- Ensure that national security, homeland security, and civil requirements receive full and appropriate consideration in the decision-making process and facilitate the integration and de-confliction of these requirements for space-based PNT capabilities.
- Coordinate individual Departments' and Agencies' PNT program plans, requirements, budgets, and policies, and assess the adequacy of funding and schedules to meet validated requirements in a timely manner.
- Promote plans to modernize the U.S. space-based PNT infrastructure, including:

  (1) Development, deployment, and operation of new and/or improved national security and public safety services when required and to the maximum practical extent.

  (2) Determining the apportionment of requirements between the Global Positioning System and its augmentations, including consideration of user equipment.
- Review proposals and provide recommendations to the Departments and Agencies for international cooperation, as well as spectrum management and protection issues.

National Space-Based PNT Coordination Office

The National Space-Based PNT Coordination Office's responsibilities that impact this plan are to:

- Provide all staffing functions for the National Space-Based PNT Executive Committee.
- Serve as the Secretariat to the Executive Committee.
- Ensure interagency transparency regarding PNT programs, policies, budgets, and mutual activities.

National Space-Based PNT Advisory Board

The National Space-Based PNT Advisory Board will operate solely in an advisory capacity as directed by the Policy and in accordance with the Federal Advisory Committee Act, Public Law 92-463, 5 U.S.C., App. The Board will evaluate national and international needs for changes in space-based PNT capabilities, assess possible trade-offs among options, and provide independent advice and recommendations to the Executive Committee on requirements and program needs. These evaluations will be considered by the Executive Committee in advising on and recommending a national PNT strategy and developing annual updates to the 5-Year Space-Based PNT Plan.

GPS INTERFERENCE

GPS and the Critical Infrastructure

The provisions made in the U.S. Space-Based PNT Policy recognize the importance of GPS and encourages its use for applications in the critical infrastructure as well as for safety-of-life applications. GPS users have seen a largely unconstrained increase in unregulated use of the civil GPS signal, which currently provides a world-wide source for PNT services to many users in multiple applications. The utilization of GPS has become widespread among sectors listed as "critical infrastructures" by the U.S. Government. Through recommendations from the DOT Research and Special Programs Administration Center (disestablished in 2005, and now the Research and Innovative Technology Administration), the transportation industry and in particular, aviation, endorsed and mandated measures establishing standards, procedures and requirements for GPS use and integration. While the criticality of safe navigation is self-evident, the use of precise timing and frequency sources is also critical to many business sectors. The U.S. Government has for some time attempted to publicize the impact of GPS interference through the efforts of the Civil GPS Service Interface Committee (CGSIC) at various events. The IDM Plan will implement a multi-layered approach to GPS interference that ensures that CI equipment is properly designed and integrated and that interference is detected and mitigated promptly.

GPS Vulnerability and Analysis Studies

Several risk and vulnerability assessments of civil GPS applications have been performed. The report published by the John A. Volpe National Transportation Systems

Center for the DOT in August 2001[6] primarily addressed the vulnerability of the national transportation infrastructure that relies on the GPS. Other assessments have identified vulnerabilities of the critical infrastructure to space-based PNT service disruptions, including interference. The body of assessments form the basis for the conclusion that GPS is fundamentally vulnerable to interference. Although not specifically referenced in the plan, many other GPS vulnerability studies have been conducted by government and private agencies.

Interference

Interference can be broadly split into two distinct categories, unintentional or intentional. Both of these are defined and described in the Volpe report along with examples of interference sources. It is important to realize that to date, interference within the U.S. has been unintentional in nature, and the process and procedures currently established deal with the reporting and mitigation of unintentional GPS anomaly events. Unintentional sources can arise from electronic devices radiating in Radio Navigation Satellite Service (RNSS) or Aeronautical Radionavigation Services (ARNS) protected frequency bands, as well as DoD interference testing activities.

Intentional interference is broadly described as deliberate attempts to jam, meacon or spoof GPS receivers. The complexity and sophistication of intentional jammers can be wide ranging. Therefore, the rapid detection, characterization, geo-location and mitigation of interference are not simple tasks, but require careful consideration and prioritization.

Redundancy and Back-up Capability

As previously mentioned, the use of GPS in civil and commercial applications is systemic and prolific in nature, being fed by the availability of inexpensive GPS receivers and access to the GPS civil signals free of direct user charges. Little guidance or consideration has been given to civil applications, outside the transportation industry, to manage standards on equipment purchased voluntarily and at the discretion of the user. Good planning and engineering should consider contingencies such as back-up systems, conventional procedures, and intrinsic equipment to ensure continuity of operations. Back-up systems do exist and can provide services dependent on the user's requirements for PNT. Under the U.S. Space-Based PNT Policy, the DHS is responsible for the coordination of back-up PNT service requirements for Homeland Security purposes. The usefulness of the back-up system is dependent on the application and requirements for PNT services, which varies dramatically from application to application. The future utility and comparison of potential back-up systems are analyzed in detail in the 2004 Radionavigation Systems Task Force Report to the Secretary of Transportation[7], along with recommendations for future studies and analysis.

[6] Vulnerability Assessment of the Transportation Infrastructure Relying on Global Positioning System, John A. Volpe National Transportation System Center, U.S. DOT, August 29, 2001
[7] Radionavigation Systems Task Force, Radionavigation Systems: A Capabilities Investment Strategy, January 2004

Mitigation

For the purposes of this document, mitigation can be defined as any action taken to permanently eliminate or reduce the long-term risk to human life, property, and function from PNT interference. To date, the primary method of interference mitigation is provided by coordinated government enforcement response to interference reports and information distribution. Outage risks can be mitigated in part if the user is aware of GPS reliance and integration, understands the consequences of system failure, conducts integrity monitoring or simulates system failure through realistic training and exercises. If this awareness of reliance and failure is evident, then the correct assessment of requirements and implementation of appropriate back-up systems or procedures for each individual application can be utilized to mitigate risk of PNT service outage.

CURRENT GPS INTERFERENCE REPORTING PROCEDURES

The use of GPS for PNT related services and information is relied upon by a large variety of systems and applications within the critical infrastructure. This reliance has led to the need to monitor the availability and integrity of civil services. Over the past years, GPS performance and interference reporting procedures have been developed and are currently provided by the U.S. Coast Guard (USCG) Navigation Center (NAVCEN), the Federal Aviation Administration (FAA) National Operations Control Center (NOCC) and the U.S. Strategic Command GPS Operations Center (GPSOC). These three core organizations collect and disseminate GPS related information as shown in Figure 4-1, providing complementary reporting, investigation status and mitigation efforts that deal with enquiries and issues from both military and civil users alike. The differing needs of the users from these three core organizations are reflected by the requirements for information that had led in turn to the development of a variety of unstandardized plans and procedures for GPS interference and anomaly reporting. The IDMP leverages all the existing governm ent

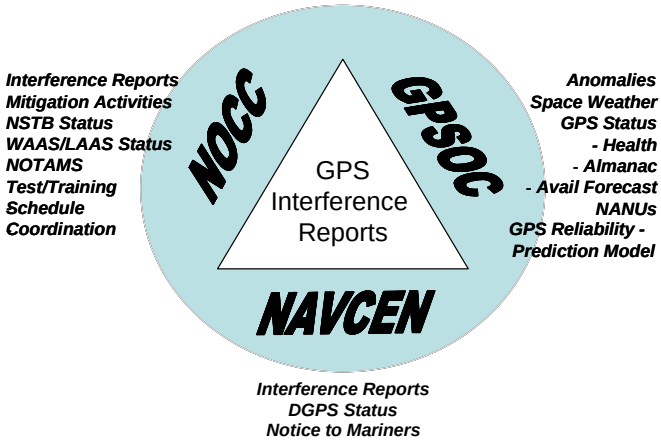

Figure 4-1. Principle Organizations

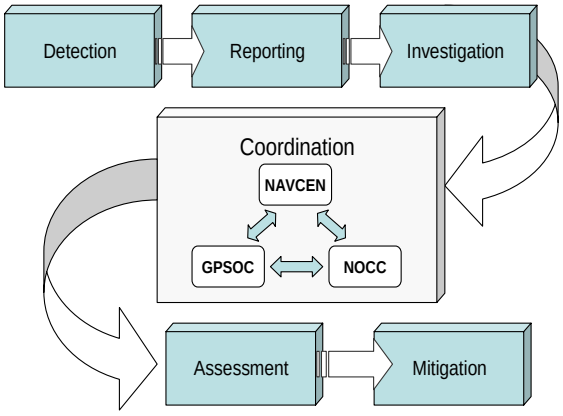

Figure 4-2. Functional Approach

capabilities, procedures and plans to streng then interagency cooperation and response to both intentional and u nintentional interference in the ev ent of a signif icant national incident or for routine reports of anom alies and outages. All the procedures follow a similar functional approach as illustrated in Figure 4-2. The major goals are the detection and reporting of the anom aly or interferen ce, investigation status, coordination of information, assessment of the impact and the application of mitigation strategies.

U.S. Coast Guard Navigation Center

General Capabilities

The USCG NAVCEN is the primary interface to all civil non-aviation users of GPS. The NAVCEN Navigation Inform ation Service (NIS) has established and m aintains a continuous point of contact (POC) that pr ovides a capability for question or issue resolution regarding GPS anom alies and interference reporting, to support maritime and land users with prioritized approach for sa fety-of-life applications. A web-based software application provides GPS and USCG augmentation systems status inform ation services. The USCG also provid es an impact assessment on the Nationw ide Differential GPS (NDGPS) du ring scheduled and unscheduled GPS outages for analysis and com parison. The NAVCEN will process all G PS user reports of outages, anom alies and signal degradation, including aviation users, and routinely forward interference reports to the GPSOC or the FAA NOCC, as appropriate.

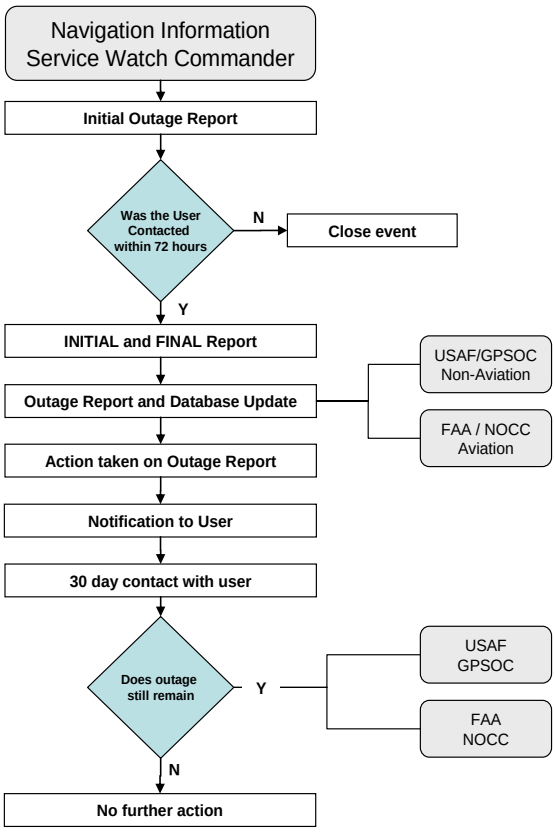

Figure 4-3. NAVCEN Interference Reporting Procedures

The overall intent is the resolution and dissemination of information, providing feedback to the users as to why service was interrupted. If an outage event is as sociated with maritime users, the GPS outage can be verified by the utilization of Coast Guard ships and assets. In addition, the NDGPS system also provides rem ote monitoring of the GPS signal (an inherent sensor for GPS signal quality) that can indicate problems or GPS outages in the vicin ity of the NDGPS stations. This capab ility provides corroboration of in terference and the recognition of significant events without exte nsive implementation of new system s. To better understand the impact of GPS interference, the USCG regularly participates in

DoD Navwar tests and evaluation exercises to evaluate the impact on maritime operations from GPS denial and interference.

Figure 4-3 shows the flow of information through the NAVCEN upon receipt of an interference report, providing information to either the FAA NOCC or GPSOC dependent on the source of the report and its potential disruption. Any aviation related outages are forwarded to the FAA NOCC for further investigation due to the safety-of-life considerations and associated responsibilities. Information is forwarded to the GPSOC to determine constellation status and impact of satellite outages or problems. The final resolution of a report is concluded by either the restoration of GPS services or the provision of an explanation of the cause of an anomaly.

Federal Aviation Administration National Operations Control Center

General Capabilities

Responsibility is allocated to the FAA for the management and resolution of all aviation reported interference. Due to the safety-of-life considerations, the FAA has well-defined procedures for dealing with the notification and coordination of any interference reports from aviation users, which includes the processing of National Airspace System (NAS) interference reports and specifically, GPS interference reports. The procedures capture the actions necessary to record a detailed interference report; identify whether the reported interference is from an approved Federal-Electronic Attack (EA) test event; coordinate a response; determine the credibility of an anomaly; distribute notification; investigate and locate sources; and coordinate mitigation to minimize as quickly as possible impact on other aviation users.

The left side of Figure 4-4 (next page) shows the FAA inter-organizational effort required to communicate the presence of a GPS anomaly impacting aviation NAS users. The procedure is designed to provide timely accurate information to the NOCC, where further investigation, analysis, coordination and assessment of impact will begin.

Continued next page

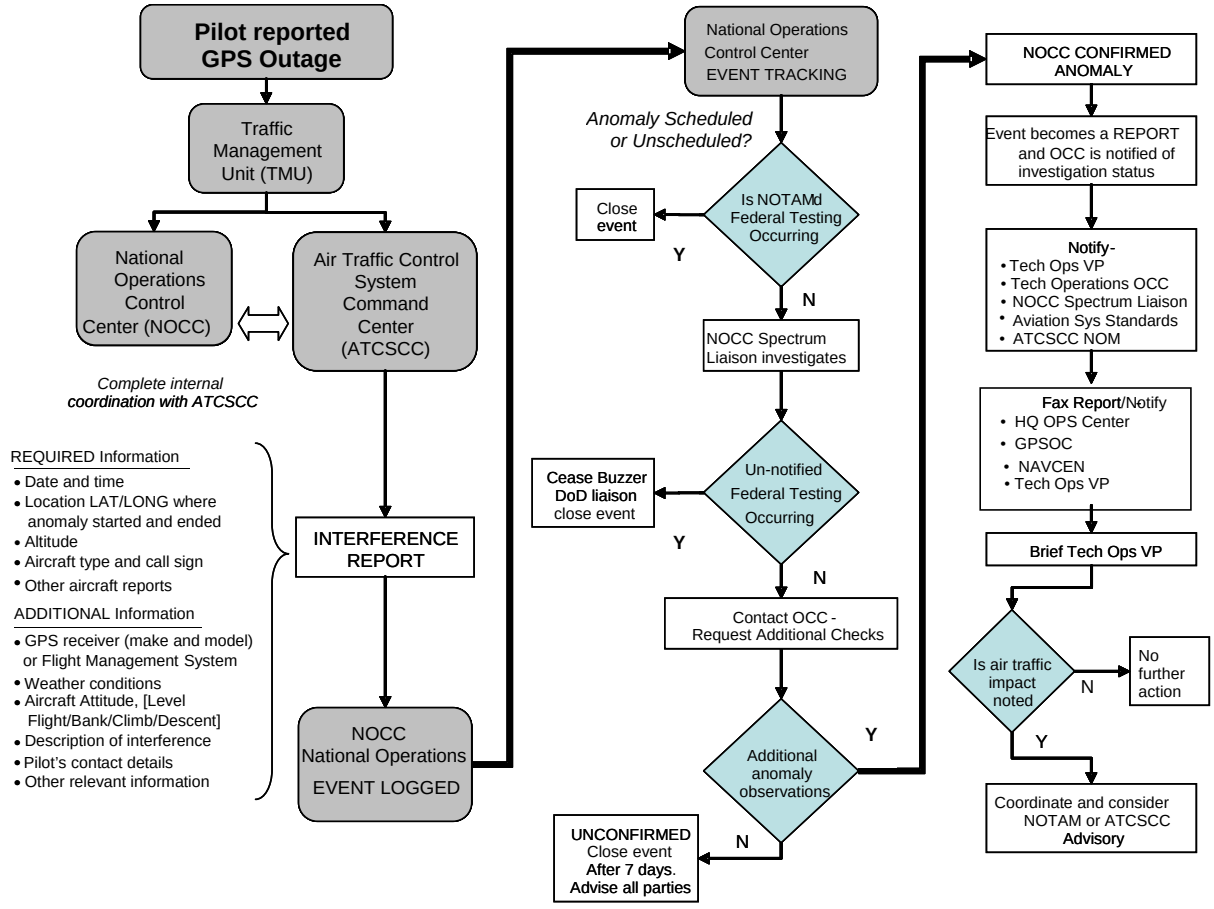

Figure 4-4. Organizational Communication and NOCC Coordination Channels

Figure 4-4 also highlights the high-level procedure once an interference event is reported and recorded. The NOCC will identify all pre-coordinated or pre-approved GPS EA and testing. If the anomaly is reported within the airspace confines of Federally approved (by NTIA or DoD) GPS EA or test operation, the anomaly is not considered interference. These events are considered approved and aviators/mariners are notified, as required, via Notice to Airmen (NOTAM) or Notice to Mariners (NOTMAR). If the anomaly report is outside an approved GPS EA or test operation, the FAA-DoD Liaison, in coordination with the NTIA, will further attempt to identify the interference source. While the FAA-DoD Liaison and NTIA verifications are ongoing, appropriate FAA spectrum personnel will research the NTIA Government Master File (GMF) database. The FAA-DoD Liaison or NTIA may contact the FCC's Communications and Crisis Management Center (CCMC) if necessary to resolve the case of interference. Once the validity of an event is determined, the incident is logged in the FAA's Event Manager and is then subject to further investigation, status suspense timelines, as well as being a mandatory briefing item to senior management until resolution. The anomaly is further examined internally to determine the cause and extent of the impact on other NAS users and augmentation

systems[8], before being notified to other agencies. The NAVCEN and GPSOC are principal organizations contacted by the NOCC once internal coordination is complete and an anomaly is verified.

U.S. Strategic Command GPS Operations Center

General Capabilities

The GPSOC is the DoD primary point of contact for information regarding status of GPS Precise Positioning Service (PPS) and GPS Standard Positioning Service (SPS), including accuracy and availability; predictive coverage/accuracy information; GPS performance history; assistance in analyzing GPS data; and generation of information to supplement reports covering analysis and findings of outages and signal degradation. The GPSOC is the focal point for the Joint Functional Component Command for Space (JFCC SPACE), to provide electromagnetic interference (EMI) assistance to DoD. The GPSOC is the interface with the USCG NAVCEN and FAA NOCC, and has the responsibility for responding to inquiries and providing information regarding the GPS constellation and the existence of space segment anomalies or issues that could result in GPS outages worldwide. The GPSOC monitors and provides data regarding PPS anomalies and interference on a worldwide basis. The GPSOC is tasked to maintain and provide limited access to a central database of GPS anomalies. This database is currently in development; however, the GPSOC accepts GPS SPS and/or PPS problem reports from the NOCC or NAVCEN to assist in the resolution of outages. Per the GPS Operations Center Concept of Operations (CONOPS), the GPSOC overarching mission is to operate, maintain, and employ GPS to produce a desired effect in support of military, civil and allied operations across the full spectrum of conflict. One of the key aspects of this effects-based concept is to provide interference detection, location and mitigation assistance. Inter-organization information is distributed by means of e-mail and web access, and accommodates both planned and unscheduled outages and anomalies. Predicted geographical impact of interference can be modeled using the GPS Interference and Analysis Tool (GIANT) application, to analyze and predict areas of interference coverage; however, the GPSOC currently has no automated data input by which to feed the modeling software. The quality of input data to the model is essential to accurately predict coverage impact and is reliant on measured assessments of interference type, location, power and altitude.

Federal Communications Commission

General Capabilities

The FCC, or Commission, is the principal organization for enforcing compliance with the Communications Act[9] that investigates violations and enforces provisions under the Act for non-Federal users of the radio spectrum. Although the FCC can issue Notices of Apparent Liability (NAL) for failure to comply with rules and regulations of the Communications Act, it does not have authority to undertake criminal prosecution. The

[8] Wide Area Augmentation System (WAAS), Local Area Augmentation System (LAAS)
[9] Communications Act, 1934 as amended by the Telecommunications Act of 1996

FCC refers criminal cases to the U.S. Department of Justice. The FCC's Communications and Crisis Management Center (CCMC) is manned 24/7 to respond to interference complaints and notifications from the general public, including GPS incidents.

National Telecommunications and Information Administration

General Capabilities

The National Telecommunications and Information Administration (NTIA) assigns frequencies to, and amends, modifies and revokes frequency assignments for radio stations belonging to and operated by the United States, makes frequency allocations, establishes polices concerning spectrum assignment, allocation and use, and provides the various departments and agencies with guidance to assure that their conduct of telecommunications activities is consistent with these policies. NTIA maintains a database of all authorized uses of radio spectrum allocated for Federal Government use. In addition, in support of the U.S. Space-Based PNT Policy, NTIA is developing the Department of Commerce Plan to determine emission limits necessary to protect spectrum used by the GPS. NTIA is responsible for investigation and coordinated resolution of interference from Government-owned systems that endanger the functioning of radionavigation or other safety critical services. Current procedures are defined in the NTIA Manual[10]. The NTIA maintains the GMF of all licensed proponents and those applying for license approval.

PNT INTERFERENCE DETECTION AND MITIGATION PLAN

The DHS was tasked in the Policy to develop a plan for coordinating U.S. interference detection and mitigation capabilities; the collection, analysis, data storage, and dissemination of interference reports; and development, implementation and exercise of procedures to request assistance from the Secretary of Defense. Sections 2-4 of the Plan reviewed various Presidential policies affecting interference detection and mitigation; Department and Agency responsibilities with respect to interference detection and mitigation; GPS interference and studies on the vulnerability of GPS and the effect on the critical infrastructure; and the current GPS interference reporting procedures, investigation efforts, and mitigation capabilities. This information provides the background for this plan, whose purpose is to leverage existing Federal capabilities, plans and procedures and to secure interagency cooperation necessary to identify, locate and mitigate sources of intentional or unintentional interference of space-based PNT services within the U.S. This section of the Plan captures the current baseline, and provides a roadmap to strengthen capabilities to meet the Policy directives. Figure 5-1 shows how the implementation of this plan will lead to an incremental development of improved capability over the near-, mid- and far-term timeframes.

[10] NTIA Manual, Chapter 8, Procedures and Principles for the Assignment and Coordination of Frequencies, Rev 1 2005 – section 8.2.30

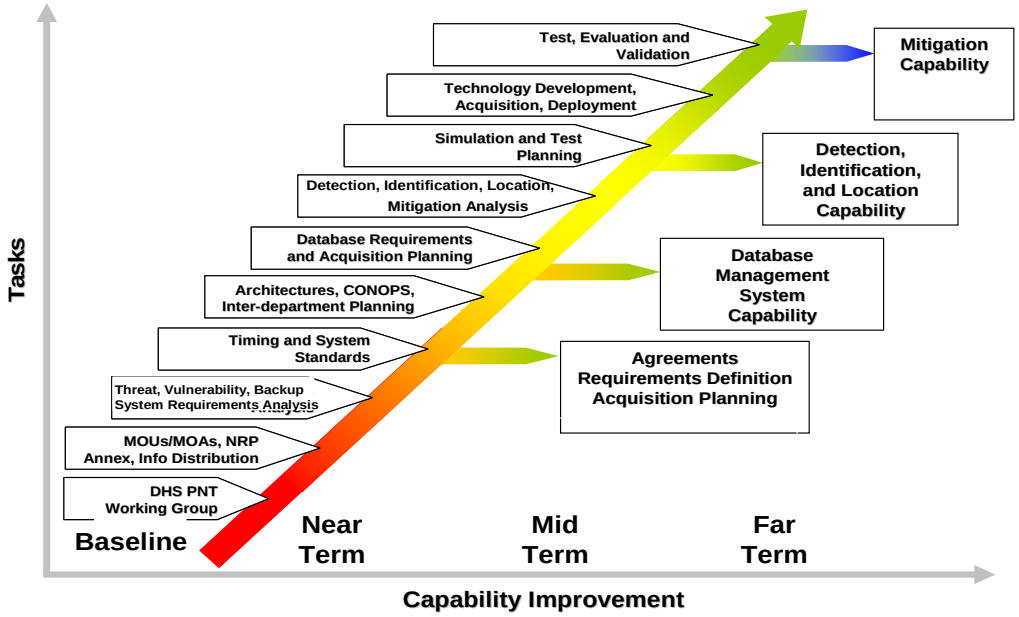

Figure 5-1 Incremental Capability Improvement

Current Architecture Overview

Current reporting procedures, investigation efforts and mitigation capabilities were described and highlighted earlier in this Fact Sheet. The procedures were developed and designed to provide a manageable system of inter-organizational cooperation and utilization of existing assets and capabilities. The current procedures meet the initial requirements for the intended objectives of notification and information distribution, concerning interference to civil users of GPS. The services provide a means to allow reporting of incidents or anomalies, investigation of the event and feedback to the user of why service was disrupted. If significant impacts are noted, further investigation and mitigation of the interference source is conducted appropriately. Each organization has distinct roles as previously defined, and plays a defined part in the resolution of such anomalies. The current plans and procedures re-route information to the organization best placed or chartered to investigate and respond.

Capability Development and Improvement

The U.S. Space-Based PNT Policy guidance gives clear direction as to what capabilities are desired to protect the use of PNT services for homeland security and other civil applications. The plan considers how capabilities can be improved to best complement and build on the existing Federal architecture and infrastructure. It is recognized that the realization of improved capability is subject to inter-department and inter-agency cooperation necessary to concur on the path to capability enhancement, inter-departmental agreements and funding allocations.

Funding for any future capability development or improvement will be the subject of a prioritized assessment of the cost versus likelihood of occurrence and impact of incidents. This plan details measures necessary to meet policy responsibilities but does not attempt to quantify the funding responsibilities or requirements. Funding requirements will become more complex through the inter-departmental coordination and cooperation required to meet many of the responsibilities. The important element is to justify and estimate budget inputs for the President's Budget. Without this financial assessment, the viability of the plan will be severely restricted.

Scope of Work and Execution

The concept of planning improvements to PNT interference detection and mitigation capability requires an understanding of the basic requirements with an estimation of the timeframe necessary to execute the capability improvement. Figure 5-1 showed how the implementation of this plan can lead to an incremental development of improved capability over the near-, mid- and far-term timeframes. This plan does not detail the specific work or solutions but the activities necessary to develop the capability. The allocation of priorities and funding will be the key drivers to successful implementation. The decisions for determining department and agency contributions or priorities will be conducted through the arrangements detailed in the inter-department or agency MOUs and MOAs, and will potentially be subject to the National Space-Based PNT Executive Committee approval.

CONCLUSIONS

This PNT Interference Detection and Mitigation Plan examined the requirements for improving capabilities within the Federal government necessary to fulfill the responsibilities detailed in the U.S. Space-Based PNT Policy and Homeland Security Presidential Directives. Based on the arguments, deliberation, capabilities, and policies outlined throughout the Plan, the following conclusions can be drawn:

- PNT services have been recognized as a component of multiple sectors of the United States critical infrastructure.

- Civil use of PNT services has been highlighted as vulnerable to interference, both intentional and unintentional. Measures necessary to prepare for, prevent, or respond to incidents that impact the critical infrastructure should undergo continuous improvement.

- Measures can be taken in a phased approach to mitigate deficiencies in capability. Measures must be coordinated and subject to inter departmental or agency agreements to establish suitable prioritization and funding to achieve coordinated objectives.

- Any approach allows for incremental capability improvement. Significant assets do exist within the Federal government that could be improved and utilized to provide a significant increase in interference detection and mitigation capability.

- Any capability improvement that is dependent on technology development must be subject to a comprehensive requirements analysis prior to subsequent investment, development, testing, and fielding.
- Vulnerability assessments, interagency agreements, plans, and fielded operational capability must be routinely exercised to ensure the adequacy and effectiveness of response measures detailed in this plan.
- The Plan took into account force structure, resource, and technology implications. Consistent with the National Infrastructure Protection Plan, Sector-Specific Agencies and other Federal departments and agencies identified have committed to work with the Secretary of Homeland Security, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to coordinate funding and implementation of actions associated with the Plan and the actions outlined in this document. New funding requirements will be addressed in future appropriations legislation.

RECOMMENDATIONS

Based on the conclusions listed above, the following recommendations are made in support of the PNT Interference Detection and Mitigation Plan:

- Establish a DHS PNT Working Group to detail the responsibilities and tasks per department, agency or other organization, necessary to execute the PNT Interference Detection and Mitigation Plan, and ensure that organizations train, test, and exercise these methods. Develop a spending plan justifying resources required to execute the near-term plan.
- Prioritize and secure funding to execute the near-term plan. Further definition and funding is required to define the schedule, milestones, and cost and risk assessment along with the subsequent execution of the inter-departmental agreements, the operational response planning documents and an information distribution plan.
- In conjunction with the DoD:
  - Support DoD efforts to integrate the Plan into their instructions and conduct exercises with departments and agencies as appropriate
  - Ensure clarity and congruency between the plan and DoD processes
  - Support DoD efforts to assess the role of the Joint Navigation Warfare Center as part of this plan
- Coordinate and complete the inter-agency MOUs and MOAs, and complete staffing and signing of all necessary agreements.
- The DHS PNT Working Group will develop and coordinate an operational response planning document with the DHS Incident Management Team.
- Coordinate informational briefings and communication of the PNT Interference Detection and Mitigation Plan's intent, content and direction in order to enable

further dissemination of information to departments, agencies, administrations, organizations and State and local authorities impacted by the Plan.

- Evaluate and coordinate the impact of mid- and long-term strategies and plans from funding, planning and risk perspective prior to any capability, requirements or acquisition planning decisions.
- Establish an appropriate coordination mechanism with the intelligence community for PNT interference detection and mitigation, as well as foreign threats to GPS.
- Coordinate threat, risk, and vulnerability mitigation efforts with other departments and agencies, building on their existing methodologies, procedures and systems.

MAINTENANCE AND REVISION

It is intended that this Plan be a living document that defines the ongoing concerns and methodology for creating a more robust capability for the detection and mitigation of interference to civil PNT services. This first version will be reviewed and be updated one year from issue. The DHS will retain control and authority over this plan, in coordination with the appropriate Executive Committee Departments and Agencies.

ADDITIONAL INFORMATION: Visit www.gps.gov