Department of Homeland Security

Agency-Specific Strategic Spectrum Plan

PROVIDED IN RESPONSE TO THE PRESIDENTIAL MEMORANDUM PRESIDENTIAL DETERMINATION: MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES ENTITLED "IMPROVING SPECTRUM MANAGEMENT FOR THE 21ST CENTURY"

U.S. Department of Homeland Security
Office of the Chief Information Officer

November 2007

Table of Contents

EXECUTIVE SUMMARY

On November 30, 2004, the President issued an Executive Memorandum directing Heads of Departments to develop agency-specific strategic spectrum plans to assist the National Telecommunications and Information Administration (NTIA) in improving the spectrum management process and in developing a Federal Strategic Plan. DHS submitted its initial Strategic Spectrum Plan in January 2006. As directed by NTIA, this updated Plan provides a synopsis of areas critical to effective management and utilization of the spectrum at the Department of Homeland Security (DHS) providing:

- An overview of DHS missions
- A summary of DHS's current use of the spectrum and anticipated future requirements
- A discussion of DHS's current and anticipated future use of commercial services and unlicensed devices
- A set of Goals, Objectives, and Strategies to guide the DHS in improving spectrum management in the future
- A discourse on particular issues of immediate concern to the Department

A separate report was prepared to address the unique missions and requirements of the U.S. Coast Guard (USCG). The report, entitled *United States Coast Guard Strategic Spectrum Plan* provides a look at current USCG spectrum use, a discussion of critical programs, and a 10-year projection of future spectrum requirements. Taken together, these plans provide a complete summary of departmental spectrum management, utilization, and future requirements.

The components of DHS are tasked with numerous law enforcement and public safety missions to ensure the protection of the homeland. As a result, the personnel within the Department rely heavily on tactical and non-tactical communications to support their day-to-day mission needs. The primary use of spectrum within the Department is dedicated to Land Mobile Radio (LMR) and Maritime Mobile Radio (MMR) networks and systems sustaining these operations. The majority of these systems operate in the Very High Frequency (VHF) band. LMR and MMR technology are the sole technologies that are able to provide the push-to-talk, security, and broadcast communications capabilities required by DHS law enforcement users.

DHS OneNet, a unified Internet Protocol platform for connecting every DHS location and all DHS mission areas, will drive DHS spectrum requirements in the future[1]. DHS OneNet supports existing mission-critical wireless data and voice systems to provide on-demand, wireless communications capabilities with appropriate levels of coverage, security, and reliability. DHS

[1] DHS Enterprise Services Division is responsible for developing the DHS OneNet Wireless Strategy and Process.

OneNet infrastructure also supports interoperability by leveraging existing Federal, State, and local systems to provide DHS users access to improved capabilities in a cost effective manner. By providing integrated wireless data and voice services, DHS OneNet further builds the capabilities to leverage modern technologies (e.g. Wireless Broadband) to increase situational awareness.

This report is considered a living document that will be updated at least biennially. DHS will continue to work closely with NTIA and other federal agencies to further refine the spectrum requirements of the Department's complex missions. The Department's plan for improving spectrum management is as follows—

1) Leverage DHS OneNet efforts to increase spectrum efficiency and effectiveness within the Department
    a) Increase shared usage of existing mission-critical wireless data and voice systems to provide on-demand, mission-critical wireless communications capabilities
    b) Develop a coordinated, Department-wide strategy for deploying enhanced capabilities that utilize cutting-edge technologies to supplement and enhance mission-critical communications and collaboration capabilities

2) Continue to integrate spectrum into the Department's enterprise architecture (EA) and planning process
    a) Ensure spectrum-dependent investments are in line with the Department's strategic goals and target architecture

3) Improve interoperability and sharing among public safety agencies at all levels of government
    a) Increase awareness of opportunities to share spectrum and telecommunications assets among public safety agencies
    b) Increase participation in and visibility of current and planned DHS sharing/interoperability programs

1.0 INTRODUCTION AND BACKGROUND

1.1 Purpose

This DHS Agency-Specific Strategic Spectrum Plan is developed as the agency response to Section 2a of the Executive Memorandum released by President George W. Bush on November 30, 2004. This Memorandum, *Improving Spectrum Management for the 21st Century*, directed the Executive Agencies to provide, to the Secretary of Commerce (National Telecommunications and Information Administration [NTIA]), an agency-specific strategic spectrum plan,

> *(a) Within 1 year of the date of this memorandum, the heads of agencies selected by the Secretary of Commerce shall provide agency-specific strategic spectrum plans (agency plans) to the Secretary of Commerce that include: (1) spectrum requirements, including bandwidth and frequency location for future technologies or services; (2) the planned uses of new technologies or expanded services requiring spectrum over a period of time agreed to by the selected agencies; and (3) suggested spectrum efficient approaches to meeting identified spectrum requirements. The heads of agencies shall update their agency plans biennially. In addition, the heads of agencies will implement a formal process to evaluate their proposed needs for spectrum. Such process shall include an analysis and assessment of the options available to obtain the associated communications services that are most spectrum-efficient and the effective alternatives available to meet the agency mission requirements. Heads of agencies shall provide their analysis and assessment to the National Telecommunications and Information Administration (NTIA) for review when seeking spectrum certification from the NTIA.*

A separate report was prepared to address the unique missions and requirements of the U.S. Coast Guard (USCG). The report, entitled "*United States Coast Guard Strategic Spectrum Plan*" provides a look at current USCG spectrum use, a discussion of critical programs, and a 10-year projection of future spectrum requirements. Taken together, the USCG Plan and the DHS Plan provide a complete summary of departmental spectrum management, utilization, and future requirements. The USCG and DHS Wireless Services (WS) work very closely to ensure the strategic plans and initiatives are consistent with DHS Guidelines.

This report is considered a living document that will be updated at least biennially. DHS will continue to work closely with NTIA and other federal agencies to further refine the spectrum requirements of the department's complex and consistently changing missions.

1.2 Mission

In January of 2003, the United States Government established the Department of Homeland Security (DHS) to unify the national effort to secure America by preventing terrorist attacks, gathering intelligence, securing the borders, and coordinating response during times of disaster. The President's *National Strategy for Homeland Security* outlined the basic purpose behind establishing the Department and provided an overview of its homeland security responsibilities. The Department's strategic goals and objectives are directly linked to accomplishing three objectives of the National Strategy—

1) Prevent terrorist attacks within the United States
2) Reduce America's vulnerability to terrorism; and
3) Minimize the damage and recover from attacks that do occur

To achieve these objectives, the Department brought together a diverse set of agencies from across the Federal Government under one umbrella. The mission requirements of these agencies necessitate continued support of current spectrum use. The components and agencies with the largest spectrum requirements are listed below with some background into each of their missions.

Customs and Border Protection (CBP) – CBP is the unified border agency within DHS that manages, controls, and protects the Nation's borders, at and between official points of entry. CBP's current mission is to prevent the entry of terrorists and instruments of terror into the United States, prevent individuals from entering the United States illegally, and curtail the flow of illegal narcotics while facilitating the flow of legitimate travel and trade.

Federal Emergency Management Agency (FEMA) – The Federal Emergency Management Agency currently supports its mission to reduce the loss of life and property, and protect the nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters by providing our Nation with a comprehensive management system of preparedness, protection, response, recovery, and mitigation.

Federal Law Enforcement Training Center (FLETC) – The Federal Law Enforcement Training Center is an interagency law enforcement training organization that seeks to provide fast, flexible, and focused training to secure and protect America. FLETC currently provides training and services to over 80 Federal agencies as well as state, local, and international law enforcement bodies.

Immigration and Customs Law Enforcement (ICE) – The U.S. Immigration and Customs Law Enforcement is the largest investigative arm within DHS, which upholds its mission for identifying and shutting down potential threats at the Nation's border, economic, transportation, and within infrastructure security.

Transportation Security Administration (TSA) – The Transportation Security Administration was created under the Aviation and Transportation Security Act with the mission to secure the Nation's transportation systems such as airports highways, railroads, buses, mass transit, and ports.

United States Secret Service – The U.S. Secret Service serves as the protection for national leaders such as the President, Vice President, and their families, and conducts criminal investigations regarding United States currency counterfeiting.

DHS Headquarters element - Science and Technology (S&T) The Directorate for Science and Technology (S&T Directorate) is the primary research and development arm of DHS.

DHS Headquarters element – Office of Investigation (OIG) The Inspector General is responsible for conducting and supervising audits, investigations, and inspections relating to the programs and operations of the Department. The OIG is to examine, evaluate and, where necessary, critique these operations and activities, recommending ways for the Department to carry out its responsibilities in the most effective, efficient, and economical manner possible.

DHS Headquarters supported element – White House Communications Agency (WHCA) DHS, USSS has historically supported WHCA with mutual aid and operational frequencies. DHS provides WHCA availability to the DHS frequency assignments and allotment pool as required to support mutual mission objectives.

2.0 CURRENT SPECTRUM USAGE

This section addresses DHS current spectrum usage and provides a summary of the types of applications being supported, spectrum management challenges, the feasibility of sharing the spectrum with Federal and Non-Federal agencies, as well as the agency's commitment to use new technologies to improve spectrum efficiency.

DHS strives to further support and enhance its key wireless communications systems, which include:

- Tactical Voice—Land Mobile Radio (LMR) systems provide communications between agency entities, and state and local first responders. The new tactical communications systems support Project 25 (P25) digital narrowband compliant, with Advanced Encryption Standard (AES) and Global Positioning (GPS) capabilities. Deployable communications kits (e.g. NOMAD kits) offer tactical voice and internet communications.

- Audio and Video Surveillance—Fixed and mobile camera surveillance systems enhance situational awareness during specific field operations, enabling authorized agencies to securely connect to the camera feeds and share video, audio, and intelligence data for command & control operations.

- Streaming Video—Integrated network video solutions provide live feed and on- demand training and communications content for identifying and shutting down vulnerabilities for each of the components. These video streaming solutions also provide DHS with mission critical video content via an Internet Protocol (IP) interface.

- Unmanned Aerial Vehicles (UAVs)—UAVs assist with border surveillance activities. These aerial vehicles use electro-optic sensors and communications payloads to provide images to field agents.

DHS is the second largest user of Federal spectrum behind the Department of Defense. The following tables and figures provide information on current spectrum usage within each component. They represent a snapshot of current frequency authorizations for each Departmental component. Table 2-1 and Figure 2-1 detail DHS's frequency authorizations by band.

Table 2-1
DHS Frequency Authorizations by Band

Component	High Frequency (HF)	Very High Frequency (VHF)	Ultra High Frequency (UHF)	Above 3 Gigahertz (GHz)	Total
CBP	1,372	5,050	645	1,180	**8,247**
Departmental Offices	101	135	130	6	**372**
FEMA	981	277	166	0	**1,424**
FLETC	0	112	7	7	**126**
ICE	6	1,184	677	19	**1,886**
IWN	0	9	0	0	**9**
OIG	0	3	0	0	**3**
Science & Technology	0	14	0	0	**14**
TSA	0	1,365	4	0	**1,369**
U.S. Secret Service	0	2,326	285	14	**2,625**
White House Communications Office	0	305	16	0	**321**
TOTALS	**2,460**	**10,780**	**1,930**	**1,226**	**16,396**

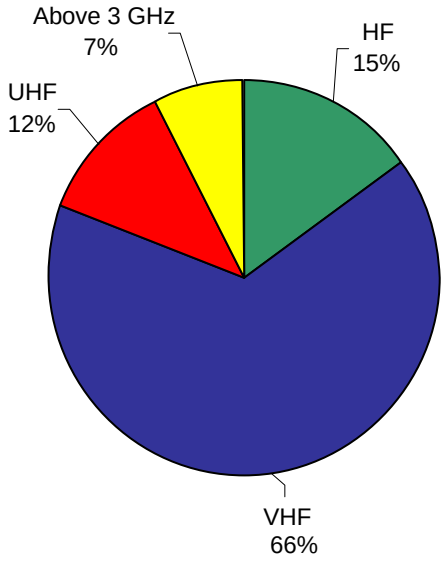

Figure 2-1
Frequency Authorizations by Band

Figure 2-2 graphically illustrates the distribution of frequency authorizations by component.

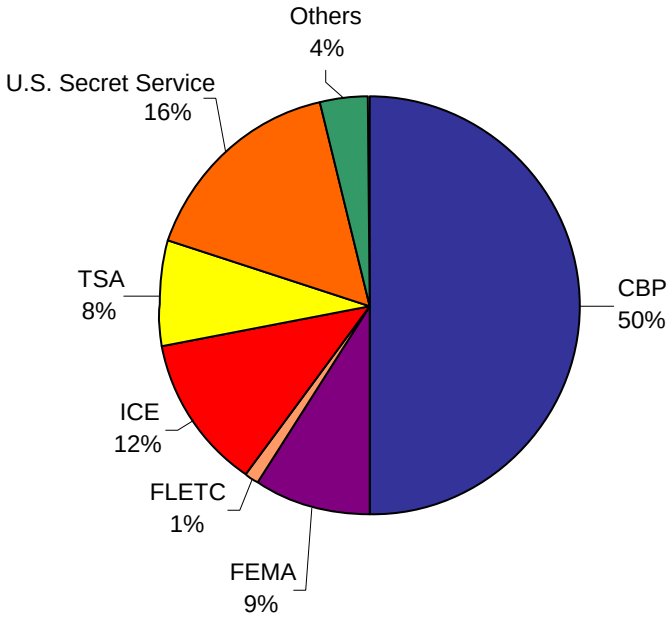

Figure 2-2
Frequency Authorizations by Component

As shown, CBP is the largest user of the Federal spectrum. There are two major factors that account for CBP's intensive use of the spectrum. First, CBP's mission is to manage, control, and protect the nation's borders, at and between official points of entry to prevent the entry of terrorists and instruments of terror into the United States. To achieve its mission, CBP relies on a number of spectrum-dependent technologies. Efforts like the Secure Border Initiative Program (SBInet) are primarily focused on transforming border control through technology and infrastructure. SBInet provides frontline personnel advantages of securing the nation's land borders through the most effective integration of current and next generation wireless communications technology, infrastructure, staffing, and response platforms. Along with tactical voice communications through LMR systems, CBP continues to support seismic, heat and motion sensor applications. These sensors are responsible for monitoring areas around canyons and mountain ranges along the northern and southern U.S. borders.

Additionally, CBP's current number of frequency authorizations does not accurately reflect its spectrum usage because of its ongoing modernization efforts. At this time, CBP has obtained frequency authorizations for several sectors of its new systems. However, these sectors are still in the implementation phase and have not yet been activated. CBP will hold double the number of necessary authorizations until the new systems have been tested, and the legacy systems have been decommissioned. CBP anticipates the modernization process to span several years, but expects to reduce the overall required number of frequencies once the modernization is completed.

Figure 2-3 graphically illustrates DHS's frequency authorizations by usage.

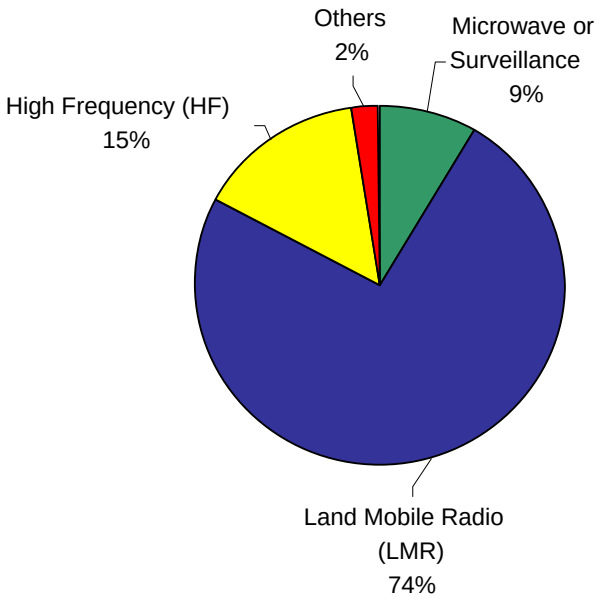

Figure 2-3
Frequency Authorizations by Usage

As shown in Figure 2-3, DHS primarily uses spectrum for LMR. Each of DHS's components relies on their tactical LMR systems for mission-critical communications. The 162-174 MHz band is the most heavily used band for LMR communications due to its propagation characteristics. FEMA relies heavily High Frequency (HF) communications to support its disaster recovery mission. ICE and U.S. Secret Service use video surveillance technologies for law enforcement purposes. CBP relies on its microwave backbone to transmit monitoring data along the nation's borders.

ICE and U.S. Secret Service are the primary investigative arms within DHS and are responsible identifying and shutting down potential threats at the nation's border; economic, transportation, and infrastructure security; and providing protection to our nation's leaders. In support of these objectives, ICE and the U.S. Secret Service combine new investigative approaches with new resources to provide investigation, interdiction, and security services to the public and to law enforcement partners in the federal, state, local, and tribal sectors. ICE provides investigative support to U.S. Secret Service for protective details, a highly visible and intensive mission during the election campaigns. ICE and U.S. Secret Service agents and officers require interoperable tactical communications and surveillance equipment to meet this mission requirement.

Very High Frequency (VHF), Ultra High Frequency (UHF), and HF frequencies are heavily used by DHS components during all phases of disasters (e.g. pre-disaster coordination, initial response, search and rescue, recovery, and post-disaster coordination) and law enforcement operations. ICE uses fixed and deployable LMR network designed to provide coverage for

enabling communications while maintaining flexibility to support peaks in service requirements for activities such as raids. This is a nationwide network, primarily focusing on the interior of the country. Due to its nomadic mission, U.S. Secret Service primarily relies on a deployable LMR network. This allows U.S. Secret Service to meet its mission without deploying an expensive, nationwide fixed network. On the other hand, CBP and TSA utilize geographically-focused LMR networks. Much of CBP's infrastructure is focused along the U.S.-Mexico and U.S.-Canada borders. TSA's infrastructure is focused at transportation hubs, such as airports.

ICE and U.S. Secret Service are also members of the DHS Technical Operations Support (TOS) program, an enterprise wide program that develops and manages procurements of technical operations surveillance equipment for department wide use. TOS's primary focus is the development and procurement of covert audio and video surveillance equipment, providing agents with state-of-the-art surveillance equipment, enhancing safety during covert operations, and improving evidence collection capabilities through the use of digital techniques. It includes not only Radio Frequency (RF) body-wire audio devices but also outdoor covert video enclosures, indoor covert video applications, ground sensors, thermal imaging and night vision equipment for low light operations, covert tracking devices (ground air and space platforms) that support logging travel activities of targets, and other wireless devices that can be used to assist agents in locating hostage takers and other criminals.

TOS coordinates the development and procurement of surveillance systems across DHS through the use of inter-bureau working groups, resulting in improved asset coordination, increasing system interoperability and comparability across the department, enabling DHS to more effectively reduce violent crime and seize illegal assets. TOS addresses, through the use of the inter-bureau working groups, issues common to all bureaus, capturing best practices, improving information sharing, and leveraging cost efficiencies from shared procurements.

CBP's border monitoring efforts rely heavily on its microwave backbone infrastructure. Due to the remote nature of many portions of the border, CBP uses microwave links to transmit data such as streaming video and sensor activations to its dispatch centers. Part of this backbone network is located in the 1710-1755 MHz band and is being relocated. Additionally, SBInet will increase the data requirements of this network. Design recommendations and bandwidth requirements are currently being established by the system integrator.

The Federal Emergency Management Agency (FEMA) currently supports its mission to reduce the loss of life and property, and protect the nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters by providing our Nation with a comprehensive management system of preparedness, protection, response, recovery, and mitigation through HF communications. FEMA currently supports the FEMA National Radio System (FNARS), Urban Search and Resume programs, as well as Mount Weather Emergency Operations Center (MWEOC) Fire and Security programs. MWEOC, operated by FEMA, primarily focuses on disaster victims seeking assistance, as well as on-site training of state and local emergency management officials. Given the potential lack of infrastructure at a disaster scene, HF's propagation characteristics are best suited for long-distance communications. The increase in

number of mission requirements along with an increase in personnel and staff have driven FEMA to seek out additional resources to continue to support mission operations and programs.

Overall, components within DHS are reinforcing their management structures to integrate spectrum and information technology to recognize and raise the importance of critical missions and operations they support. The ability for components within DHS to prevent threats against the United States is achieved through monitoring and surveillance along key points of entries, which include borders, ports, and waterways. To fulfill and continue supporting these critical operations DHS must heavily rely on wireless communication systems and a variety of new emerging technologies that are spectrally efficient.

3.0 FUTURE SPECTRUM REQUIREMENTS

DHS OneNet, a unified Internet Protocol platform for connecting DHS locations and all DHS mission areas, will drive DHS spectrum requirements in the future. DHS OneNet supports existing mission-critical wireless data and voice systems to provide on-demand, wireless communications capabilities with appropriate levels of coverage, security, and reliability. DHS OneNet infrastructure also supports interoperability by leveraging existing Federal, State, and local systems to provide DHS users access to improved capabilities in a cost effective manner. By providing integrated wireless data and voice services, DHS OneNet further builds the capabilities to leverage modern technologies (e.g. Wireless Broadband) to increase situational awareness.

Under the DHS OneNet vision, components are beginning to follow these principles to modify and modernize their end-state wireless communications capabilities. These principles and wireless communications capabilities are captured in the DHS Wireless Communications three-pronged strategy[2]:

- Upgrade and Modernization – Replace aging subscriber and infrastructure equipment with digital, narrowband P25 equipment

- Leverage Existing Networks – Leverage commercial services to enhance capabilities and develop policies and standards to provide technical and operational guidance required by interoperability

- Build Integrated Data and Voice Capabilities- Transition to integrated broadband solution for DHS data and voice communications

The following section addresses DHS future spectrum requirements by general technology category. The Department will continue addressing future needs in subsequent updates and editions of this plan. As previously noted this is an evolving document and will be updated as DHS mission needs and spectrum requirements change.

3.1 Land Mobile Radio and Tactical Voice Communications

Land Mobile Radio (LMR) remains the predominant wireless communication technology used by DHS, with more than 74% of current frequency assignments directly supporting LMR operations. Additional spectrum, such as microwave links connecting repeater sites, indirectly supporting it. LMR is the sole primary technology currently used at the Department, which provides the push-to-talk, security, and broadcast communications capabilities required by DHS law enforcement users. LMR will continue to remain a critical asset to DHS missions and users in the future.

[2] DHS Enterprise Services Division is responsible for developing the DHS OneNet Wireless Strategy and Process.

DHS is currently undertaking several modernization efforts led by ICE and CBP to increase spectral efficiency by converting to narrowband operations. New tactical voice communications systems supporting DHS components are P25 digital narrowband compliant and possess advanced features such as GPS capabilities. These efforts support NTIA's narrowbanding mandate, and provide officers and agents with modern communication capabilities.

The ICE Atlas Modernization Program will include the collective modernization and upgrade of the Special Agents in Charge (SAC) Offices (Figure 3-1) nationwide. This upgrade includes the transition of subscriber equipment to digital narrowband AES encrypted and P25 compliant tactical communications equipment and is projected for FY 2009 through FY 2013. To complete the modernization within the specified time-frame, ICE will need access to additional spectrum resources over the next five to ten years. This modernization effort will replace aging legacy portable radios and systems that are beyond their current life cycle, do not meet current mandates for encryption, do not provide interoperability, and do not support current mission requirements.

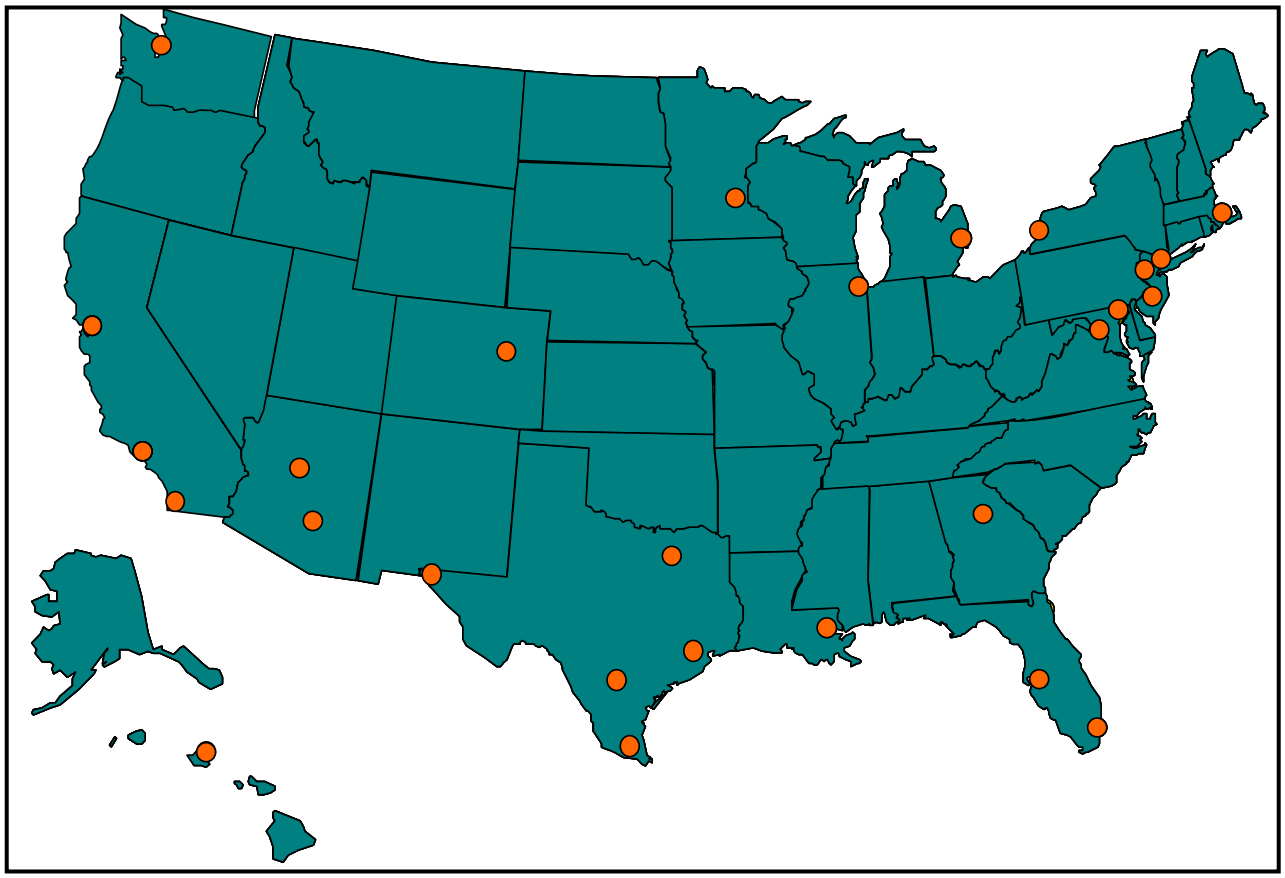

Figure 3-1
ICE SAC Office Locations

The goal of the Atlas Program is to acquire sufficient subscribers (e.g. a combination of mobiles, portables, and base stations) and infrastructure, and deploy them in designated ICE SACs in response to urgent, mission critical requirements. The radios and systems will be deployed to

high priority areas where ICE agents and officers routinely require interoperation with (1) the U.S. Secret Service in support of protective details, and (2) CBP. At this time, approximately 50% of subscribers have been upgraded to digital, narrowband capable, P25, AES encrypted equipment. Delays in receipt of investment funding have delayed ICE's modernization efforts for its systems and infrastructure.

CBP is also undertaking a large-scale modernization effort for its LMR system implementing narrowband digital technologies on a sector by sector basis. CBP is currently installing new equipment in its Tucson and Yuma sectors. Houlton and El Paso sectors are the next priority and thus will be ugraded next. Figure 3-2 identifies the CBP sectors. CBP expects this to be a multi-year project but actual timeline depends on funding and the ability to work several sectors concurrently. Once completed, CBP anticipates a decrease in the total number of frequencies used by its LMR systems and a significant decrease in the actual required bandwidth.

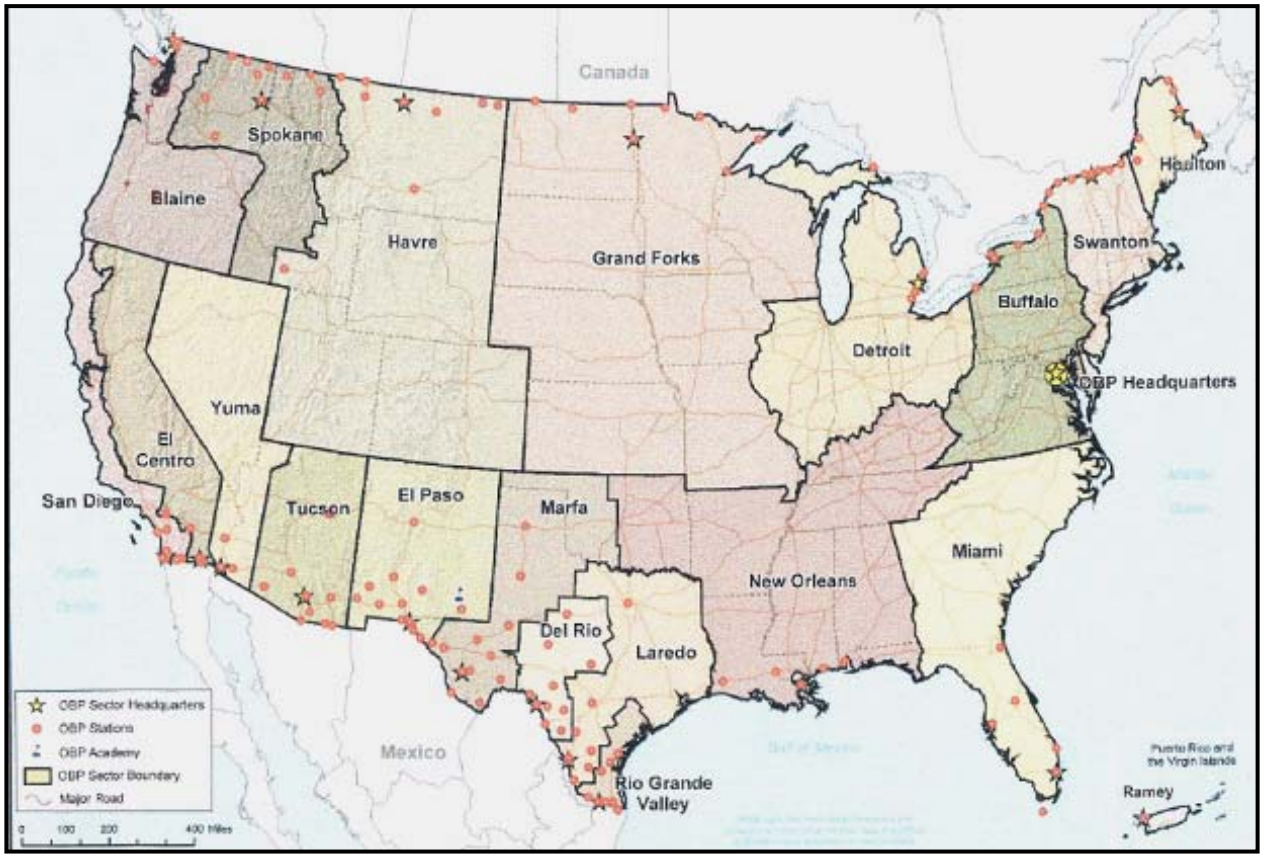

Figure 3-2
CBP Sectors

CBP and ICE are coordinating their designs and deployments to ensure that they are compatible and will provide enhanced capacity for agents and officers operating in the area. To the maximum extent possible, the infrastructure will be collocated, sharing lease space and rack space to minimize redundancy and costs. The subscribers will be programmed with each

component's respective frequencies as well as with interoperable frequencies and encryption keys.

FEMA anticipates additional LMR based equipment in the VHF and UHF bands will be needed in the next two to five years. These issues have raised concern due to FEMA's borrowing of VHF frequency assignments from the Department of Defense (DoD). FEMA anticipates these frequencies may affect critical missions and operations because they may be recalled by the DoD at any time.

DHS anticipates that it will continue to see significant growth in its officer and agent corps. The continued expansion of mission and responsibilities for each component, along with the increase in the number of agents, officers, and vehicles, will require (1) upgrades of existing systems to support the increased traffic; (2) expansion of existing systems to support the increased geographic areas of responsibility; (3) deployment of mobile data capabilities; and (4) increased spectrum allocations to support these requirements.

One of the key realizations that DHS will get from these efforts, is the ability to collaborate with other Federal departments and agencies and with State, local, and tribal partners across the country. Interoperability is an integral requirement for systems and spectrum to support day-to-day interoperability, task force interoperability, and incident (emergency response) interoperability. Effective interoperability provides a horizontal (Federal-to-Federal), as well as a vertical (Federal-State-local-tribal), solution to meet DHS mission critical requirements.

3.2 Audio and Video Surveillance

DHS continues to support the use of covert audio and video surveillance equipment to field agents and law enforcement officials. The number of users who support this equipment has grown at approximately 3-10% per year. Sustained growth in the years to come will be contingent upon Congressional approval and the availability of spectrum funding. Across all the components, the need for surveillance technology is expected to increase by 25% in the next five to ten years. Investments in new audio and video surveillance equipment will be coordinated through the TOS.

One major change to the audio and video surveillance spectrum usage will be the transition from analog to digital transmissions. At this time, numerous pieces of surveillance equipment operate in the 1710-1850 MHz band. DHS will be transitioning out of the 1710-1755 MHz portion of the band by March 2008 to provide access to new commercial Advanced Wireless Services (AWS) providers. Due to its transition timelines, DHS will continue to use analog equipment in the near term. DHS is planning to convert to digital equipment once suitable covert digital equipment has been developed. DHS expects that this conversion will be financed by the AWS Transition fund. The conversion to digital technology will increase the spectral efficiency of DHS's audio and video surveillance operations.

3.3 Streaming Video

Streaming video is currently employed for ICE, U.S. Secret Service, and CBP covert applications to allow agents to view potential threats remotely to enhance their on-going investigations and minimize the chance of detection. CBP continues to deploy infrared and daylight cameras across the Mexican and Canadian borders to scan for potential threats (e.g. drug runners and illegal immigrants). The latest generation of ICE-TV enables employees to receive video programming on their desktop. The broadcasts can be received both on-demand and in real-time.

In the future, ICE is interested in implementing streaming video that can be transmitted to cellular phones and Blackberry's as the technology becomes available. These services will require additional wireless network infrastructure and increased bandwidth on the public network.

3.4 HF Networks

DHS uses three individual HF networks: COTHEN, FNARS, and the U.S. Coast Guard HF network. In recent years, the importance and utility of these networks and the need to ensure continued and expanded spectrum support has been underscored dramatically during times of emergency and heightened alert. Emphasis on improved emergency preparedness and continuity of government planning also has placed increasing importance on enhancing support to these networks. Since HF has significant international implications, both in cross-border protocols and at the International Telecommunication Union (ITU), DHS considers support of emerging HF requirements to be of primary significance to future mission support.

Emerging HF systems have new spectrum requirements. These enhanced technologies include—

- **Electronic messaging systems (E-mail)—**HF electronic messaging networks often provide numerous ground entry points throughout a region or around the globe. These ground entry points are interconnected by the Internet to central message servers. Remote users establish an HF link to any suitable entry point to send and receive their messages. HF electronic messaging systems often use specialized protocols over the air.

- **Interactive internet applications—**In contrast to electronic messaging, other HF Internet applications are more interactive. Users expect nearly instantaneous responses to their input (typing or mouse clicks). Such applications include Web browsing, remote login, and instant messaging (sometimes called "HF chat").

- **Large file transfer access—** Files of hundreds of kilobytes ('large' files) are sent via HF easily and often. However, due to the limited bandwidth of HF radio links, multi-megabyte files are rarely sent via HF. Operational limitations must be taken into account when conducting large file transfers that occupy a link for extended periods.

- **Software defined radios with the technical capability to operate over HF—**The migration of protocols away from the physical layer and toward the transport and session layers has proved to be a complementary trend toward interfacing with the network, data-link and physical layer functions of Software Defined Radios (SDR). In fact, the High Speed HF modem and other physical and data-link layer devices are already planned as intended capabilities in some future software defined radios.

- **Digital voice—**Digital voice technology offers two key features: improved intelligibility compared to analog voice in the presence of moderate channel impairments, and the ability to encrypt the voice stream for privacy.

3.5 Microwave

DHS uses microwave links to transmit data between fixed points. In the past, DHS components have used a number of frequency bands including 900 MHz, 1710-1850 MHz, and 7125-8500 MHz. Currently, CBP is relocating several microwave systems out of the 1710-1755 MHz band to clear the band for commercial AWS operations. CBP is examining a number of options including other federal fixed bands appropriate for point-to-point links, government-owned fiber networks (i.e., dark fiber), and commercial networks. The 7125-8500 MHz band will be the primary destination for most of the relocated links. Additionally, to support the SBInet Program, CBP anticipates the installation of microwave broadband (30-40 MHz) systems along the northern and southern borders during the next five to ten years. In many cases, these new broadband systems will replace existing, lower-capacity systems.

DHS anticipates that commercial fiber will increasingly be identified as the optimal backhaul solution for connectivity of tactical communications within the next five to ten years. DHS will continue to rely on Federally-allocated spectrum to support these needs where other technologies or services are not available or do not fit the mission requirements.

3.6 Broadband Data Networks

In recent years, technology has advanced to the point where Federal, State, and local public safety officials can envision transmitting very high speed data (referred to as Broadband, from 1 to 10 Mbps) such as live video, large files, complex documents and images, and other applications in short time periods and to a number of fixed and mobile devices. DHS and its public safety partners foresee a number of missions that will require spectrum-dependent broadband applications for internal DHS functions as well as shared integrated broadband systems for interoperability purposes. Effective regional and wide-area broadband systems may require as much as 30 MHz of spectrum to support, in bands less than 1 GHz.

4.0 CURRENT AND FUTURE USE OF NON-FEDERAL SPECTRUM OFFERED BY COMMERCIAL SERVICE PROVIDERS

4.1 Current Use of Commercial Services

DHS currently uses commercial services to provide wireless voice and data communications for non-mission critical applications. These commercial wireless services include Commercial Mobile Radio Service (CMRS), commercial satellite telephony, commercial wireless data services, and commercial microwave/fiber data services. Commercial services are selected when they provide the most cost-efficient option and meet mission and policy requirements. Service providers include the following:

- Verizon
- Sprint/Nextel
- AT&T
- T-Mobile
- Iridium
- Global Star
- InMarsat
- Directwave

CMRS technology is extensively used throughout the Department for administrative purposes. Most components issue mobile data devices (i.e., Blackberry) to their management level staff. This allows for the key decision makers to remain in contact with the office regardless of their current location. Additionally, several components such as ICE and U.S. Secret Service issue cellular phones to their agents for administrative use. FEMA uses CMRS technology for dispatching and communications with convoys in route to disaster areas. FEMA's NOMAD kits also include a CMRS router for deploying commercial data network. These applications minimize the amount of non-mission critical traffic on the components' licensed networks. U.S. Secret Service also uses location-based commercial services (i.e., LoJack) for tracking applications.

FEMA has implemented Inmarsat's Broadband Global Area Network (BGAN) satellite uplink terminals for NOMAD kits to provide additional tactical voice communications and e-mail applications support. The NOMAD kits allow portable mobile communications that transmit and receive voice, video, and real time data through a single deployable device. Currently these kits have not yet been deployed and used in a disaster-type situation; however they have been tested and used during numerous simulations. The number of kits deployed to an incident scene depends on the type of disaster and FEMA's urgency for immediate portable incident emergency command, control, and communications capabilities. In the future, FEMA expects to use these kits' built-in Ku-band satellite service during catastrophic events.

FEMA has noted some difficulties during its simulations with capacity related issues. At times, additional NOMAD kits have not be able begin operations due to the number of users on the

system. FEMA is working with Inmarsat to identify methods to alleviate these capacity issues. Potential solutions include dynamic allocation of more capacity to meet the user demand.

4.2 Future Use of Commercial Services

In discussions with its components, DHS has identified three major issues which have limited the implementation of commercial services: security, reliability, lack of ubiquitous coverage areas, and priority access. As these issues are addressed in the future, DHS expects its usage of commercial services to increase significantly. These services will primarily be used to support non-mission critical communications, such as administrative functions. Due to the safety-of-life nature of many mission critical communications, DHS and its components are hesitant to embrace current commercial technologies for these applications due to the following three concerns.

1. Security is one of the major concerns cited by DHS components as being a barrier to increased usage of commercial services. Since many of the components missions involve law enforcement, security for mission critical communications is a priority. At this time, services such as CMRS do not provide the necessary security features such as encryption. Until encryption is implemented at a cost-effective price-point, commercial services will most typically be used to supplement government-owned systems.

2. Reliability and coverage area is another major barrier to implementation. Since commercial systems are designed to maximize profit, they do not have the same reliability and coverage area requirements as government-owned systems. There remain significant pockets where no service is available, particularly in rural areas and along the borders. This lack of service limits the usefulness of commercial services to components such as CBP whose primary operations exist in areas of poor coverage. Additionally, commercial services are not always available during the time of need. Events such as Hurricane Katrina have shown that commercial networks are susceptible to outages during disasters. Other performance issues such as lack of capacity or dropped calls limit the utility of these networks for mission-critical DHS users.

3. Priority access is the final major barrier to the adoption of commercial services. While some programs such as the Government Emergency Telecommunications Service (GETS) and Wireless Priority Access (WPA) exist to provide priority access, it is not a universally implemented. In times of emergency, significant increases in demand by Federal and public users may result in lack of network resources. In these conditions, without priority access, Federal users will be denied service and will be unable to access the network resources.

As discussed by the Federal Communications Commission's (FCC) Independent Panel on Hurricane Katrina, the general public relies heavily on CMRS services for communications during a disaster and its recovery. CMRS is often the most reliable method for contacting persons who have relocated or sought emergency shelter. Implementation of priority access allows Federal or higher priority users access to network resources before granting resources to lower priority users or the general public. This reduces the amount of resources available for the general public attempting to contact disaster victims. DHS recognizes the emotional impact on

disaster victims and their need for commercial CMRS services in these situations. Therefore, CMRS services may not be an appropriate commercial resource to support Federal disaster response.

DHS expects its usage of commercial wireless services to continue to increase as new applications become available. However, commercial services will continue to primarily support non-mission critical communications until advances in commercial wireless services aligning to law enforcement and DHS requirements for reliability, security, coverage, and priority access. One area of key interest to DHS is the public-private partnership proposed by the FCC for public safety broadband communications in the 700 MHz band. This partnership has the potential to provide interoperable public safety broadband communications for Federal, state, and local public safety agencies. DHS will continue to monitor the regulation and implementation of this network to identify opportunities for incorporation into DHS OneNet.

5.0 CURRENT AND FUTURE USE OF "NON-LICENSED" DEVICES

5.1 Current Use of Unlicensed Devices

Currently DHS has limited usage of devices that operate in unlicensed spectrum. Two key issues have limited the deployment of these technologies: the potential for interference and security. Since unlicensed devices are governed by FCC Part 15, they have not been granted any interference protection. This limits the type of unlicensed applications that DHS can consider. Additionally, due to the large number of Departmental security requirements, such as wireless intrusion detection, auditing, transmission encryption, and policy enforcement, DHS components have been hesitant to implement unlicensed devices such as Wireless Local Area Networks (WLAN). The MD 4300A Sensitive Systems Handbook and Attachments (Q1 – Wireless Systems, Q2 – Wireless Personal Electronic Devices, and Q3 – Tactical Systems) are the DHS wireless security policies that drive implementation of wireless technologies.

The current largest deployment of unlicensed devices is the FEMA NOMAD units. As discussed previously, the NOMADs are used to establish communications at the scene of a disaster. An 802.11g router is included to establish a wireless network for FEMA responders. This router is then connected to the commercial satellite backhaul to provide network access. Although the NOMADs have not yet been deployed in a disaster response, FEMA anticipates using the network for administrative purposes such as filing situational reports and requesting additional resources. This capability will be a valuable tool for maintaining a common operating picture for disaster responses. Unlicensed devices are well-suited for this type of application given the potential lack of functional telecommunications infrastructure in disaster response situations.

5.2 Anticipated Future Use of Unlicensed Devices

The components have expressed an interest in deploying WLANs for wireless internet access in their offices. CBP is also examining the possibility of using unlicensed technology in SBInet. Unlicensed spectrum could be used to connect peripheral devices such as sensors and remote cameras within the network. One major policy decision that may be required before this type of application is deployed involves the use of unlicensed spectrum for safety-of-life operations. DHS is awaiting the recommendations from the SBInet integrators on the type of technology that will be identified to connect the peripheral devices to the network.

DHS has developed a WLAN pilot program to assess "best of breed" implementations and to identify best practices and required modifications to the Departmental security requirements. The program currently is evaluating switched WLAN, bridge WLAN, and wireless remote access through pilots.

The switched WLAN pilot extends TSA network connectivity in conference rooms, cafeteria, and other public areas at TSA headquarters. TSA has selected an integrator and equipment vendor for this pilot. At this time, the integrator has completed lab-based testing and is preparing to conduct building surveys. DHS anticipates that the system design document and equipment

installation will be completed by November 2007. Field deployments are scheduled to begin in January 2008.

The bridge WLAN pilot is examining IEEE 802.11 and millimeter wave systems to wireless connect networks between buildings at two TSA locations. This pilot is currently in the developmental stages.

The wireless remote access pilot provides remote access to the DHS Secure Wireless Access Prototype (DSWAP) over commercial Wireless Wide Area Networks (WWANs). The DSWAP prototype was developed and verified as a proof-of-concept in May 2007. The system integrator was selected in September 2007. DHS anticipates that the system design document will be completed in December 2007, and expects to begin deploying end-user applications in February 2008.

DHS expects an increase in the number of unlicensed devices being deployed. Some components are already in the process of engineering WLANs pending the outcome of the pilots. Additionally, as technologies in the unlicensed marketplace continue to expand, DHS will continue to evaluate technologies for potential applications in supporting its missions.

6.0 NEW TECHNOLOGIES

DHS's components continually seek out and evaluating new emerging wireless communications technologies for their application in mission critical operations. A critical priority of any wireless system and infrastructure is security. DHS remains a strong proponent for secure tactical wireless solutions, wireless data and multimedia, and integrated systems that support IP infrastructure. Components consider potential applications for access to broadband data, situational awareness, and other critical operations during the development of new and enhanced services. The primary interest is using portable emerging wireless technologies to promote efficiencies in investigation, interdiction, and security services to the public safety, as well as federal, state, and local law enforcement.

DHS strongly encourages components to share wireless communications knowledge and information with one another to promote efficiency and cost savings. Reliable and protected wireless technology provides DHS components with continuous access to timely intelligence, logistics, and investigative information regardless of their location. Components have also been planning and evaluating Worldwide Interoperability of Microwave Access (WiMAX) solutions, which will provide wireless data over long distances from point to point links to full mobile cellular type access. DHS is committed to procuring new and proven wireless technologies that have been tested in the field and are reliable and secure.

Due to DHS's heavy reliance on LMR technologies, compatibility with the existing, proprietary infrastructure is still a major barrier to the implementation of these new technologies. Several components with proprietary LMR systems have expressed concern that they may not be compatible with new emerging technologies. Life cycle costs and ability to work with existing legacy infrastructure must be considered before implementing and procuring new technologies. For example, the TOS Program faces compatibility and cost issues when considering enhanced surveillance technologies to augment in-house proprietary surveillance equipment (e.g. body-wire audio and video devices, thermal imaging and night vision). Additionally, DHS components are concerned about implementing new technologies, which are currently not covered by NTIA regulations (i.e., cognitive software defined radios).

Some additional challenges and barriers that must be considered when implementing and deploying new technologies include –

- Funding availability
- Existing legacy equipment interoperability
- Equipment availability
- Equipment performance in a specific environment
- Security policies
- Training or re-engineering required to use the equipment

7.0 STRATEGIC SPECTRUM PLANNING

7.1 Spectrum Management Organization

The functional roles and capabilities of spectrum management and policy currently reside within the DHS Under Secretary for Management office. Wireless Services within the Office of the Chief Information Officer (OCIO) have been charged with executing these duties. Figure 7-1 shows the organizational location of spectrum management and policy within DHS.

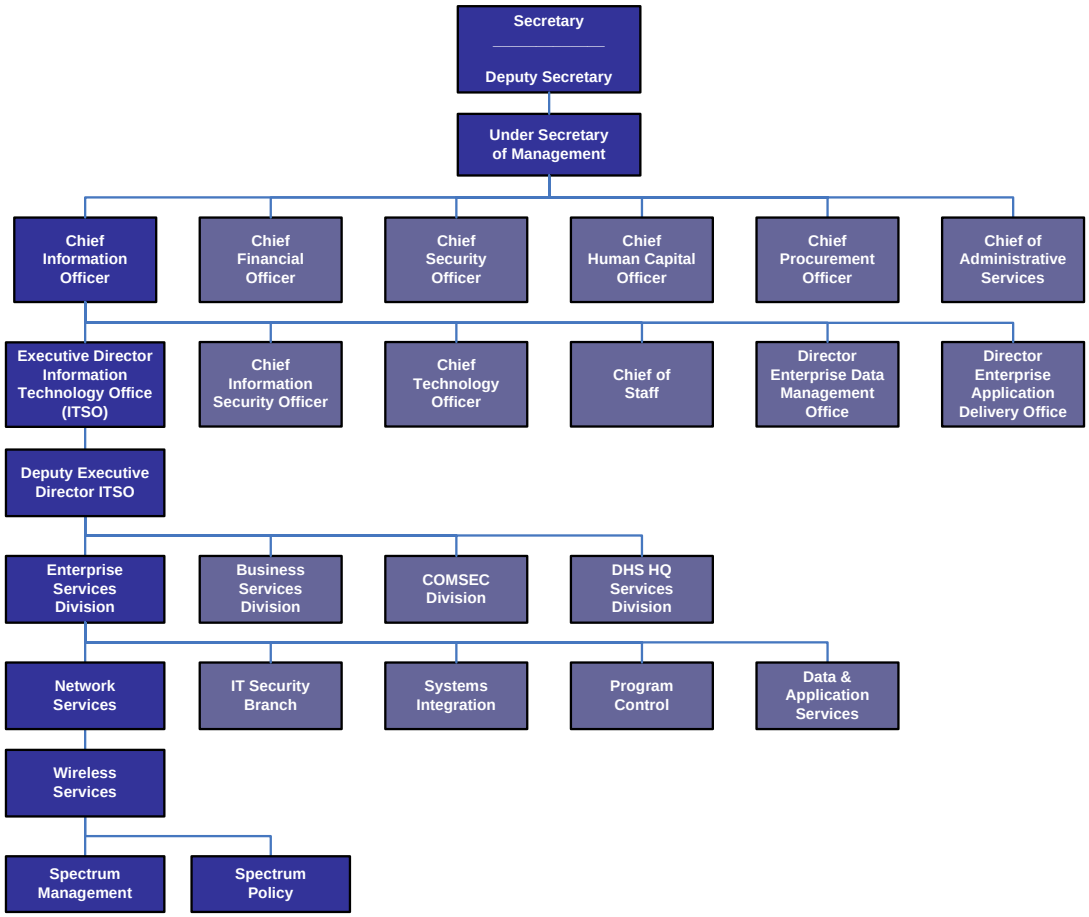

Figure 7-1
DHS Organization for Spectrum

As shown, spectrum management is integrated into the overarching IT organization. This integration helps to ensure spectrum requirements are identified in the early stages of new IT programs and systems development. Spectrum also has close ties to the enterprise architecture and capital planning processes within the Department.

This organizational structure helps DHS make significant strides to further incorporate spectrum into the capital planning, budget, and enterprise architecture processes. DHS currently uses its OCIO Acquisitions Review to evaluate major spectrum-dependent systems before funding is allocated. For the purposes of OMB Directive A-11 Section 33.4, DHS defines a major any investment over $2.5 million dollars. Included in this process is an enterprise architecture review. This ensures that new systems are in compliance with the Department's enterprise architecture and do not duplicate existing capabilities; both wireless and wireline. This process ensures that spectum is used efficiently and effectively throughout the Departmental.

7.2 Strategic Spectrum Planning

DHS has incorporated strategic spectrum planning into the existing system certification and frequency authorization process. Since most changes in spectrum usage are being driven by new or modified mission requirements, DHS has found this to be an effective method. Figure 7-2 below depicts the DHS's strategic spectrum planning process.

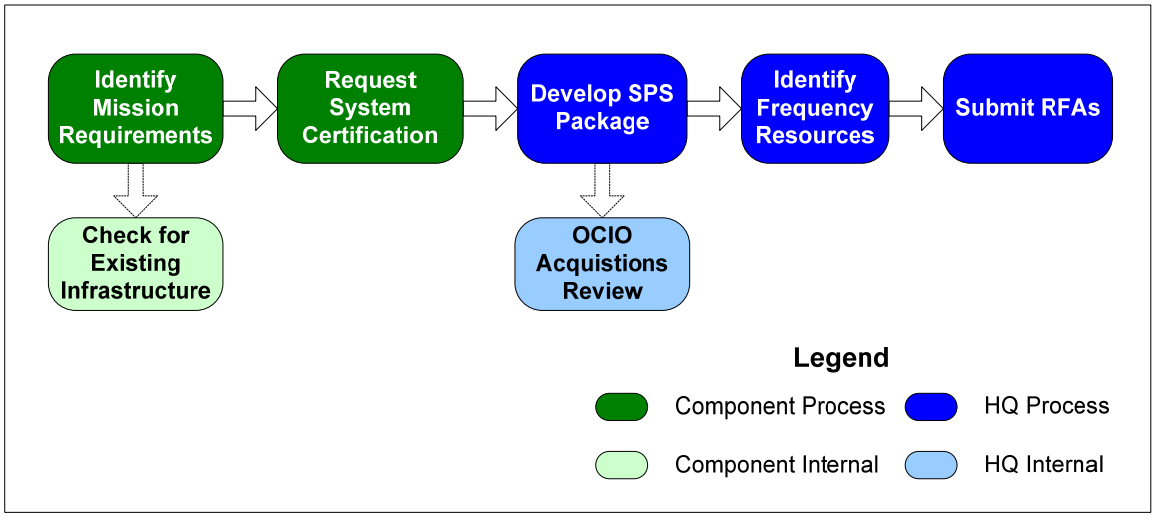

Figure 7-2
DHS Strategic Spectrum Planning Process

The strategic spectrum planning process begins when new or modified mission requirements have been identified. At that time, the affected component determines which technologies will best address the need and if they require spectrum. Components also check internally within DHS for any existing infrastructure or systems that could be leveraged in support of these requirements. Once the component has determined that it must build or expand a system to meet these requirements, it contacts Wireless Services to identify potential frequency bands and request system certification.

In coordination with the component, Wireless Services develops the certification package for the Systems Planning Subcommittee (SPS). Concurrently, the proposed system undergoes the OCIO Acquisitions Review which includes an evaluation for EA compliance. Once the system has been certified, Wireless Services works with the component to identify available frequency

resources. Wireless Services develops the requests for frequency authorizations (RFAs) and submits them to the Frequency Assignment Subcommittee (FAS) agenda.

7.3 Strategic Goals

The DHS Strategic Spectrum Vision for this new era of spectrum management within the Department is:

> *To effectively meet the needs of an ever-changing Information Technology and Wireless Telecommunications environment by supporting the immediate spectrum requirements of current services, the evident growth of existing systems, and the future needs of emerging technologies and services.*

These goals and corresponding objectives and strategies are actionable in the immediate future and are considered first steps to improving spectrum support to the vital missions of DHS. The goals, objectives, and strategies for improving DHS spectrum management are listed below.

GOAL 1: Leverage DHS OneNet efforts to increase spectrum efficiency and effectiveness within the Department

Objective 1: Increase shared usage existing mission-critical wireless data and voice systems to provide on-demand, mission-critical wireless communications capabilities.

Strategy 1: Identify key wireless systems and wireless-dependent programs being coordinated within the Department

Strategy 2: Develop strategies to leverage key wireless systems and wireless programs for use by multiple DHS components

Objective 2: Develop a coordinated, Department-wide strategy for deploying enhanced capabilities that utilize cutting-edge technologies to supplement and enhance mission-critical communications and collaboration capabilities

Strategy 1: Identify common communication requirements among components and the technologies best suited to meet these needs

Strategy 2: Leverage commercial services and unlicensed devices when feasible and cost-effective and procure them via Department-wide contracts to reduce costs and increase compatibility

GOAL 2: Continue to integrate spectrum into the Department's enterprise architecture (EA) and planning process

Objective 1: Ensure spectrum-dependent investments are in line with the Department's strategic goals and target architecture.

Strategy 1: Ensure all major spectrum-dependent systems undergo the OCIO Acquisitions Review.

Strategy 2: Encourage components to conduct reviews similar to the Acquisitions Review or, at a minimum, EA reviews on non-major spectrum dependent systems.

GOAL 3: Increase interoperability and partnerships with other Federal and Non-Federal Agencies

Objective 1: Increase awareness of opportunities to share spectrum and telecommunications assets among public safety agencies.

Strategy 1: Foster collaboration with the Office of Emergency Communications (OEC), the Federal Partnership for Interoperable Communications (FPIC), and the Office of Interoperability and Compatibility (OIC)/SAFECOM in developing strategies and plans for interoperability and sharing of spectrum and telecommunications assets among public safety agencies.

Strategy 2: Partner with regional, state, and local public safety agencies to capitalize on opportunities to share spectrum and other resources for the purpose of increased interoperability among all levels of government.

Objective 2: Increase participation in and visibility of current and planned DHS sharing/interoperability programs.

Strategy 1: Support DHS and other federal interoperability programs and pilots that highlight planning, sharing, and the use of technology to improve interoperability among public safety agencies.

Strategy 2: Publicize results of programs and pilots internally and externally.

8.0 ADDITIONAL RECOMMENDATIONS

Many factors not under the direct control of DHS affect the pursuit and implementation of the Department's plans. These include, but are not limited to:

- Budget and fiscal constraints
- Classification restraints
- Lack of usable spectrum for future plans
- Lack of regulatory flexibility to accomplish goals
- Congressional or Administrative redirection
- Changes in the commercial service environment
- International treaties

In addition to these broad issues, there are several specific issues that DHS believes NTIA can address to assist the Department in implementing its plans. These issues include interoperability, the existing LMR channel allotment plans for the LMR bands, and the accuracy of Government Master File (GMF) records.

8.1 Interoperability

The varied missions of DHS dictate that its different agencies and components interoperate with all federal agencies and many state, local, and tribal governments and public safety providers. Since the days of Public Safety Wireless Advisory Committee (PSWAC), federal agencies have strived to improve the way in which public safety agencies at all levels of government interoperate.[3] From its formation, DHS has continued to stress the importance of enhanced interoperability and formed the Federal Partnership for Interoperable Communications (FPIC) to address issues common to all public safety agencies. DHS views interoperability needs on three levels:

- **Day-to-day** interoperability to satisfy the need for routine federal-to-federal interaction as well as federal-to-state-to-local-to-tribal coordination and assistance.

- **Task Force** interoperability to address the requirement for coordinated activities of multi-government operations.

- **Disaster and Emergency Response** interoperability to accommodate the special needs of local, regional, or large-scale emergencies.

One method to obtain all three levels of interoperability is the development of shared systems. As budgets for wireless communications infrastructure and the availability of spectrum continue to decrease, shared systems provide an excellent opportunity for Federal agencies to increase

[3]The Public Safety Wireless Advisory Committee (PSWAC) was the first-ever comprehensive look at the complex issues relating to public safety communications and is recognized as the genesis of recent programs relating to telecommunications interoperability.

their networks in a spectrum and cost-efficient manner. Of particular interest to DHS is shared Federal and non-Federal networks. State, local, and tribal public safety agencies are beginning to develop regional or statewide networks. These networks can be leveraged by Federal agencies to increase their footprint without having to build a completely new network.

At this time, Federal agencies can join these systems by paying subscriber fees or by contributing infrastructure such as tower locations. As Federal use of these shared systems continue to grow, it would be advantageous for agencies to be able to contribute frequencies to expand the systems. This would result in a system using both Federal and non-Federal frequencies to support Federal and non-Federal users. At the present time, the process for regulating such a system is poorly defined.

It is unclear if Federal agencies can currently contribute frequencies to such a shared system. Each agency receives an allotment of frequencies in the LMR bands that they have priority when designing a system and requesting frequency allocations. In this case, a participating agency would essentially be obtaining the frequencies for use by other non-Federal agencies. This would limit the number of frequencies available to other Federal agencies in the given area. Since the Federal agencies do not receive an authorization for a particular frequency until it is slated to be used in a Federal system, it is unclear if a Federal agency can contribute frequencies to a shared system.

Also, the process for obtaining a frequency authorization has not yet been clearly defined. Since these systems would utilize both Federal and non-Federal frequencies, they would be governed by both the FCC and NTIA. While processes currently exist to address many sharing situations, this instance has not been specifically addressed. DHS recognizes that NTIA has already begun to examine these issues and fully supports these efforts. DHS believes that the use of shared systems will continue to grow and clear regulatory procedures will encourage the deployment of these spectrum and cost-efficient systems.

8.2 Channel Allotment Plans

Overall, DHS expects the number of LMR frequencies it utilizes to increase in the future as the number of staff supported by the system increases. These systems are the primary methodology for mission-critical voice communications and the number of users is expected to increase as DHS's components continue to add personnel. However, several components have noted difficulties in obtaining LMR frequencies within the DHS allotment pool. Due to the large number of systems DHS has in these bands, allotted frequencies are not always available for use. As a result, DHS is often forced to rely on frequencies allotted to other agencies. This bartering requirement delays the implementation of mission-critical communications systems as DHS tries to find and receive approval for the use of alternate frequencies.

To address this situation, DHS requests NTIA review the effectiveness and equity of the current LMR channel allotment plans and examine alternate allotment strategies. Agencies have different spectrum requirements based on the geographical location of their systems. Some agencies, such as the Department of Interior, primarily require frequencies in rural areas while

other agencies, such as the Department of Justice (DOJ), have concentrated requirements in more urban areas. The current channel allotment plan does not recognize these differences in missions and their resulting spectrum requirements. DHS feels that the current allotment plan does not have enough flexibility, resulting in agencies being forced to barter to locate enough frequencies to deploy mission-critical communications systems. Additionally, an agency may find, upon a change in mission, allotted frequencies in a given area have already been loaned to other agencies.

DHS recommends examining the possibility of increasing the pool of un-allotted or All Government Agencies (AGA) frequencies. These frequencies, available without footnotes to restrict their use, would provide agencies with additional options without infringing on another agency's allotment. To obtain these frequencies, DHS suggests reducing the number of frequencies allotted to each agency. For example, NTIA could reduce the number of allotments for each agency by 25%. In turn, NTIA could strongly recommend that agencies use frequencies in the un-allotted pool before resorting to using those allotted to another agency. This would reduce the number of frequencies being used outside of their given allotment and potentially streamline the frequency identification process.

8.3 Accuracy of GMF Records

As the intensity of Federal spectrum usage increases, the accuracy of the GMF will become more critical. DHS notes that NTIA has already undertaken several initiatives to increase the accuracy of the GMF. Of particular impact is the enforcement of the five year review process. By ensuring that agencies review their records at set intervals, outdated records are removed and typographical errors are more likely to be identified. DHS applauds and supports NTIA in these efforts. However, DHS has noticed a perception issue surrounding the accuracy of GMF records.

When discussing spectrum management issues with its components, DHS repeatedly heard about the perceived inaccuracies within the GMF. Components stated that old records that have not been updated or used in years were cluttering the GMF and hampering their ability to identify available frequencies. Components were not aware of NTIA's increased emphasis and enforcement of the five year reviews. DHS suggests highlighting these efforts in current and future NTIA spectrum management training events. This would help eliminate the perception that the GMF is full of inaccurate and out of date records.

As NTIA migrates to the Future Spectrum Management System (FSMS), DHS suggests that the GMF data is subject to review before transitioning to the new system. The purpose of this review is to identify typographical errors to prevent them from being carried forward into FSMS. Data mining techniques will be used to identify records, which may contain typographical errors in fields such as power and emission designator. Additionally, a mapping program may be used to determine if the provided geographical coordinates align with the city and state. These simple checks can help reduce the number of common errors in the GMF. Additionally, these checks could also be used before new records are added in the future.

APPENDIX A: ACRONYM LIST

AGA	All Government Agencies
AES	Advanced Encryption Standard
AWS	Advanced Wireless Systems
BGAN	Broadband Global Area Network
CBP	Customs and Border Protection
CMRS	Commercial Mobile Radio Service
COG	Continuity of Government
COOP	Continuity of Operations
COTHEN	Customs Over the Horizon Enforcement Net
DHS	Department of Homeland Security
DOJ	Department of Justice
DoD	Department of Defense
DSWAP	DHS Secure Wireless Access Prototype
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
FNARS	FEMA National Radio System
FPIC	Federal Partnership for Interoperable Communications
FSMS	Future Spectrum Management System
GETS	Government Emergency Telecommunications Service
GHz	Gigahertz
GMF	Government Master File
GPS	Global Positioning System
HF	High Frequency
ICE	Immigrations and Customs Enforcement
IP	Internet Protocol
IRAC	Interdepartment Radio Advisory Committee
ITU	International Telecommunication Union
IWN	Integrated Wireless Network
KHz	Kilohertz
LMR	Land Mobile Radio
MHz	Megahertz
MWEOC	Mount Weather Emergency Operations Center
NTIA	National Telecommunications and Information Administration
OCIO	Office of the Chief Information Officer
OIC	Office of Interoperability and Compatibility
OIG	Office of Inspector General
P25	Project 25
PSWAC	Public Safety Wireless Advisory Committee
RF	Radio Frequency
RFA	Request for Authorization
SAC	Special Agent in Charge
SBInet	Secure Border Initiative Program

SDR	Software Defined Radio
SPS	System Certification Process
SSP	Strategic Spectrum Plan
TOS	Technical Operations Support
TSA	Transportation Security Administration
UAV	Unmanned Aerial Vehicles
USCG	United States Coast Guard
USSS	United States Secret Service
UHF	Ultra High Frequency
VHF	Very High Frequency
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPA	Wireless Priority Access
WS	Wireless Services
WWAN	Wireless Wide Area Network
WWG	Wireless Working Group