Department of Homeland Security
Management Directive System
MD Number: 4800

TELECOMMUNICATIONS OPERATIONS

1. Purpose

This directive establishes the Department of Homeland Security (DHS) policy for Telecommunications Operations.

2. Scope

This directive applies to all DHS organizational elements.

3. Authorities

This directive is governed by numerous Executive Orders, Public Laws, and national policy, such as:

A. Telecommunications Act of 1996; The Information Technology Management Reform Act (ITMRA) also known as the Clinger-Cohen Act.

B. TITLE 47 Code of Federal Regulations, Telecommunications Parts 0-199.

C. OMB Circular A-130 Management of Federal Information.

D. Paperwork Reduction Act of 1995.

E. Government Paperwork Elimination Act (GPEA).

F. Federal Property Management Regulations (FPMR).

G. DHS MD No. 4100, “Wireless Management Office”

4. Definitions

A. ***FED-STD-1037C***: 1996-Glossary of Telecommunications Terms

B. ***National Information Systems Security (INFOSEC) Glossary***: NSTISSI No 4009 June 5, 1992.

5. Responsibilities

A. ***The DHS Chief Information Officer (CIO)*** shall:

1. Develop DHS department wide policies and procedures to ensure the efficient and effective procurement, management and operation of all telecommunications equipment, systems and services as they pertain to homeland security.

2. Oversee formulation, submission, allocation, and execution of the consolidated DHS telecommunications budget.

3. Ensure that all DHS telecommunications activities are combined into one integrated operation, with the exception of classified and unclassified systems.

4. Ensure cost effective use of commercial telecommunications technology and its integration into the existing inventory of DHS Information Technology equipment.

6. Policy and Procedures

A. ***Policies***. It is the policy of DHS that:

1. All organizational elements and agencies in DHS will function under the same policies, regulations, standards and rules pertaining to telecommunications operations.

2. All DHS organizational elements at official points of entries into the United States shall have interoperable or single telecommunications system(s) that will enable effective communications and ensure coordinated support of homeland security operations.

3. The DHS CIO will coordinate and submit to the DHS Chief Financial Officer, a consolidated DHS telecommunications budget. Organizational elements, directorates and/or agencies will receive a yearly allocation of funds for telecommunications operation and maintenance based upon annual telecommunications spending plans reviewed by the CIO. All DHS organizational elements will ensure the accurate execution of telecommunications spend plans which shall include expenditures for personnel, equipment, and maintenance.

4. All DHS civilian personnel serving in telecommunications and wireless positions (Series 0391/0301/2210, telecommunications specialists/frequency managers/ telecommunications standards) will adhere to the provisions of this directive.

5. All DHS operational elements and agencies are directed to notify the DHS CIO of any new telecommunications initiatives to ensure compliance with DHS

telecommunications and interoperability goals.

B. ***Questions or Concerns Regarding the Process***: Any questions or concerns regarding this directive should be addressed to the Office of the CIO.

Frequently Asked Questions (FAQs)

What is telecommunications?

Telecommunications refers to any technology, service, system, or other resource that provides or ensures transmission of electronic data and information. Telecommunications resources may be voice and data networks, wireless services, high speed data communications, telephones, network servers, switches, or any other device, service or system used in the transmission of electronic communication. The location of telecommunications is equally diverse, ranging from local or building networks to global networks, from single telephone handsets to communications satellites, whether dedicated to a specific application or shared by many users, programs, and applications.

Telecommunications, as defined above, which constitutes or is part of a system must be considered an Information Technology System, for all planning, acquisition, policy, security, and functional purposes.

Within this policy no distinction is made between voice-centric and data-centric telecommunications, unless specifically noted.

What is this guideline and to whom does this policy apply?

This guideline establishes policies and outlines relevant procedural guidance related to the acquisition, management, use, and disposition of telecommunications resources within the United States Department of Homeland Security and applies to all operating units of the Department of Homeland Security, including the Office of Secretary.

Why is a policy on telecommunications required?

Telecommunications resources for the Department of Homeland Security form one of the most essential elements in the operations of the agency, and it is vital that these resources be effectively managed. The Department of Homeland Security relies on telecommunications systems and services to support the mission and goals set out by the Secretary of Homeland Security, including providing the most effective service to our public and Government customers. Telecommunications is an information technology resource of immense importance to the accomplishment of work in today's Department of Homeland Security. Telecommunications allows Homeland Security operating units a degree of technological effectiveness, access and coverage unknown only a few years ago. It is therefore incumbent on all managers and employees of Homeland Security to utilize telecommunications resources to the greatest extent possible.

As valuable as they are to the mission of the agency, however, telecommunications services in themselves have become comparatively inexpensive. Their value as an asset to increase productivity has grown tremendously. Management of telecommunications resources, therefore, should be proactive in ensuring that telecommunications benefits, such as speed, usefulness and availability of services, are emphasized even while steps are taken to manage associated risks and costs. Before constraints are placed on application and use of telecommunications technologies, enlightened value judgments should be exercised to ensure the cost effectiveness of limiting telecommunications use.

Prior to 1996 and the implementation of Clinger-Cohen telecommunications policy derived from the Federal Information Resources Management Regulations (FIRMR), the Federal Property Management Regulations (FPMR) and the Federal Acquisition Regulations (FAR). For the most part, these have been superseded by:

1. The Government Performance Results Act (GPRA);

2. The Telecommunications Act of 1996, the Information Technology Management Reform Act (ITMRA), also known as the Clinger-Cohen Act;
3. The Paperwork Reduction Act of 1995;
4. The Government Paperwork Elimination Act (GPEA);
5. OMB Circular A-130.

These laws and directives serve as the foundation for development of policy and management of Federal information technology, including telecommunications.

In addition, the current government-wide policy on telecommunications management is found in the Federal Property Management Regulations (FPMR). It should be noted that during FY 2003, these policies are being revised. The DHS policy is consistent with the draft revised FPMR, which will be published as the Federal Property Regulations (FPR).

What planning for telecommunications is required?

The acquisition and use of telecommunications resources, as a subset of IT Resources, must be included in the IT planning and IT acquisition processes. Since telecommunications resources are acquired and used in response to a strategic need or requirement, these resources, as systems or groups of systems, should be considered during development of IT architectures, IT planning, and IT acquisition. Telecommunications resources should never be acquired without consideration of the use and the ways in which the telecommunications will support and enhance the mission of the agency or program.

How do we acquire telecommunications resources?

Acquisition of telecommunications services and products should be conducted in accordance with the provisions of Department of Homeland Security Procurement Manual (TBD) and the Federal Acquisition Regulations (FAR). The IT planning process must be followed, as well, for larger systems and acquisitions. See the IT Management Handbook Acquisition and Disposal section (TBD) for information on the IT acquisition planning process.

Generally, telecommunications resources should be acquired in a manner that ensures that the minimum acquisition resources are expended. Department of Homeland Security operating units should use or consider blanket or broad ranging, existing contractual programs, many of which have been competed and from which services may be easily acquired.
Numerous acquisition vehicles, contracts, and agreements, are available which meet these criteria, including the Washington Interagency Telecommunications System (WITS), Metropolitan Access Acquisitions (MAA), and many offerings from the Federal Technology Service (FTS), along with others. Most have been fully competed by either the General Services Administration (GSA) or by other agencies, which offer their programs to DHS.

Are there contracts or services which DHS offices are required to use?

Some programs are mandatory for use or mandatory for consideration by offices of the Department of Homeland Security. One of these is FTS2001. This includes FTS2001 for lease of all Land Mobile Radio Equipment and turnkey systems.

a. FTS 2001:

FTS2001 is a broad, Government-wide contract for provision of primarily long distance and international telecommunications connectivity services. It also includes local connectivity services. There are two primary considerations regarding the use of FTS2001: FTS2001 is mandatory for use within the Department of Homeland Security; and, only specifically Designated Agency Representatives (DARS) may place orders for services from FTS2001.

The Department of Homeland Security entered into an agreement with Sprint for FTS2001. This contract is mandatory for use by all offices of Homeland Security, although exceptions may be granted, using the following process, when it is in the best interests of the Government.

Non-Use of DHS Delivery Order Number TBD Under GSA Contract Number GS00T99NRD2001 For Services Within the Scope of Contract and Delivery Order

Contracting Officer: TBD
COTR: TBD

Original date of Non-Use policy: TBD

General:

The scope of Department of Homeland Security acquisition Delivery Order Number TBD is all long distance and international telecommunications for the U.S. Department of Homeland Security, its bureaus and operating units that are offered by Sprint. The scope is not limited to those services offered under the Government-wide contract number GS00T99NRD2001. The Delivery Order specifies that DHS and its bureaus and operating units will acquire all long distance and international telecommunications from Sprint for the performance period of the contract.
As a result, most long distance and international services that are acquired by the Department of Homeland Security and its operating units and bureaus fall within the scope and should be acquired from Sprint. If it is felt that acquiring these services from other than Sprint is in the best interest of the Government, prior to acquiring such services it is necessary to obtain approval for an exception to the use of this Delivery Order.

The following guidelines should be used prior to acquiring "within scope" products or services from other than Sprint.

Procedures:

Full DHS documentation of requirements must be performed. As with any other acquisition, this should specify both the functional and operational requirements for the service or product.

A business case should be developed which outlines the preferred acquisition methodology and any reasons, which, in the view of the requesting office, seem to justify acquisition outside the use of Sprint. DHS documentation must include both technical and economic analysis of the requirement, comparing Sprint information to that of the preferred acquisition source(s). Specific information should be included on why a program feels an exception is in the best interest of the government.

This DHS documentation and business case should be sent to the CO or the COTR (shown above). The COTR should forward a copy to the CO, if needed. Before acquisition from any source other than Sprint can be made, a decision in favor of exception must be made by the Contracting Officer and notification must be received by the requesting office.

It is essential that every effort be made to satisfy the terms and spirit of the Delivery Order. However, every effort will also be made to process a request for exception quickly and expeditiously. As soon as a decision is made, correspondence will be sent to the requester and the requesting office.

How to apply for an exception: The form for assignment of Designated Agency Representative (DAR) is shown as Attachment A.

B. Designated Agency Representatives

Anyone who is assigned the responsibility of Designated Agency Representative (DAR) must attend three training courses, since these employees are acquisition officials, though with limited authority. The required courses are:

DAR Training;
COTR Training, and;
Simplified Acquisition.

The FTS2001 vendor, currently Sprint, provides DAR training. COTR training may be taken from many sources, but must be a 40-hour course. Simplified Acquisition may also be taken from many sources, but must include the following topics: Contract Administration, Past Performance, and Delivery Order Procedures.

Designated Agency Representatives (DARs) should have specific assigned responsibilities and those should be reflected in their performance plans. Responsibilities and guidelines are shown in Attachment B.

Are there constraints for using telecommunications resources?

Government acquired telecommunications resources are intended for the purpose of performing the mission of the U.S. Department of Homeland Security and its operating units. With the exceptions discussed in this policy, such resources should be used in compliance with laws and regulations that apply to all Government IT resources. These resources are for the use of the Government in conduct of official business, unless otherwise determined to be in the best interest of the Government. The Chief Information Officer and telecommunications managers are responsible for effectively managing the use of telecommunications resources to ensure that the business of the Government, within their mission area, is carried out effectively and efficiently.

May Government employees be compensated for use of their own telecommunications resources?

Government employees may be reimbursed for the use of their own, privately owned, telecommunications services when no acceptable Government-owned service is available and when to do so is in the interest of the Government. In all such cases, the employee's management must approve reimbursement. Employees may not be required to acquire or use privately owned services for the purpose of performing their official duties. Employees may, however, with their own consent and with the approval of management, use privately owned resources on a repeating basis, when it is in the interest of the Government to do so. Reimbursement must be for the actual cost of the service, not an estimated or "flat" amount.

Some example applications of this policy are:

1. An employee who travels away from the office, locally or long distance, and uses a cellular device for official communications, such as a cell phone, may be compensated for the actual cost of that usage.

2. An employee who, at the request of management, works from home or away from the office may be reimbursed for the cost of telecommunications services incurred in such work.

May Government telecommunications resources be used in private residences?

Generally, Government-provided telecommunications services will not be made available in private residences. However, in support of specific programs, security, or "work at home," it is permissible to provide equipment or services where it is in the best interest of the Government to do so. Examples of permissible equipment or services might be: telecommunications modems, fax equipment, high-speed data lines, wireless services, additional voice lines, or telecommunications devices for the deaf (TDD). Examples of programs or activities which might be in the best interest of the Government are: national security, homeland security, approved work-at-home programs, or work-at-home for a handicapped employee.

Operating units may use appropriated funds to install telecommunications lines, equipment, or services and to pay monthly charges, in any private residence of an employee who has been authorized to work at home in accordance with established OPM or Commerce guidelines. These vary with operating unit. OPM guidance on steelwork, telecommuting and other work/life matters can be found at:

OPM Telecommuting/Telecommuting
OPM Work/Life Site

Work at home circumstances may also vary widely from one case to another. Therefore it is the responsibility of the operating unit CIO to establish any appropriate guidance regarding telecommunications in private residences and to apply any guidance and standards equitably.

In all cases, the operating unit CIO must grant approval of such programs or provisions and any other appropriate authority determined by the operating unit. Approval should be granted based on need and best interest of the Government. The CIO must ensure that adequate safeguards are in place to ensure that such services are placed and used in compliance with other regulations and laws pertaining to the use of Government-owned property and services, that there is no misuse or abuse of these resources, and that resources are returned to the Government after termination of the requirement.

May telecommunications resources be used for other than official Government business?

Government voice-centric telecommunications services (including cellular and other wireless services) are intended for the conduct of official business or limited personal use as outlined in this DHS document. However, employees are authorized to use these services for other than official Government business subject to the constraints of this policy. Authorized calls may include emergency calls and calls that the agency determines are acceptable in the interest of the Government.

Supervisors are responsible for the proper management of telecommunications service usage by employees and others under their jurisdiction.

The use of wireless technology does not preclude the agency's responsibility for inventory control, billing accountability, and appropriate acquisition process. For purposes of this policy, wireless services are treated no differently than other telecommunications services and equipment. They should be managed as any other resource, consistent with their unique attributes and capabilities.

Specific criteria for authorized personal use of telecommunications resources for other than official Government business are that the use:

Does not adversely affect the performance of official duties by the employee or the employee's organization;
Is of reasonable duration and frequency;
Reasonably is made to allow the employee to continue performance of work, or;
Is provided for in a collective bargaining agreement.

Examples of Authorized Use. Some examples of authorized use by employees that are consistent with the previously stated criteria are:

Calls to notify family, DHS etc., when an employee is injured on the job;
Calls to notify family of a schedule change while traveling on Government business and delays occurring due to official business or transportation;
While traveling on Government business, a call to his or her residence (but generally not more than an average of one call per day);
Calls to advise his or her family of changes in schedule or to make alternate transportation or child care arrangements;
Calls to locations within the local commuting area to speak to spouse, minor children, or other family members whose "close association" constitutes a "family relationship" (or those responsible for them, e.g., school or day care center);
Calls to locations within the local commuting area that can be reached only during working hours, such as local Government agencies or physicians, or to arrange for emergency repairs to his or her residence or automobile.

Long Distance Usage. Personal long distance usage that must be made during working hours may be made over the commercial long distance network if the call is consistent with previously stated criteria. Generally, other personal long distance usage should be made using an alternative payment methodology, such as:

Charged to the employee's home phone number or other non-Government number (third number call); or
Made to a toll-free (800, 877, 888, etc.) number; or
Charged to the called party if a non-Government number (collect call); or
Charged to a personal credit card or prepaid debit card.

Prohibitions. The following practices are specifically prohibited:

Use of Government telecommunications services for other than official business, except as provided above;

Use of any Government provided telecommunications service, equipment, or facility for usages which are permitted in the criteria but significantly interfere with the conduct of Government business;

Placing unauthorized telecommunications usage with the intent to later reimburse the Government;

Use of toll-based or similar calling services, which place a toll burden on the Federal Government.

Collect Telephone Calls. Generally, collect calls (calls placed from a non-Government number to a Government number, reversing charges) and third party calls are prohibited except for official business. A personal emergency call may be accepted without authorization, but should be reported to a supervisor. In mission locations and offices where a "call-in" capability is required, the use of a Government provided toll-free (such as “800") services should be considered.

How do we manage telecommunications resources?

Telecommunications management is an active process composed of systems, services, policies and programs that ensure that telecommunications resources are acquired, installed, used, and disposed of wisely, effectively, and efficiently.

Levels of telecommunications management for which operating units are responsible.

Operating units of the Department of Homeland Security are responsible for the management of telecommunications resources in just the way they are for the management of any other resource. In addition, there are specific requirements, as stated below.

Operating units will establish internal procedures to manage telecommunications fraud, waste and abuse of their IT resources. Operating units should also implement cost-effective procedures and systems to minimize exposure to abuse. Examples of such procedures would be the review and verification IT services billing information and education of employees on acceptable use policies.

NOTE: As stated earlier, telecommunications services should be viewed as an asset, not simply an expense liability. Before constraints are placed on usage or funding is expended on constraining employees and management, a value judgment should be made to determine the cost effectiveness of a program.

The Department of Homeland Security Chief Information Officer will:

1. Establish policy and procedures for the management and cost control of telecommunications services and systems;

2. Provide management or oversight of programs and functions which the CIO deems necessary;
3. Provide advice and assistance to operating units and staff offices regarding telecommunications services and facilities; and
4. Serve as liaison for telecommunications related activities and interchange between Department of Homeland Security and other Government-wide agencies, including the National Communications System (NCS) and functions dealing with national security and emergency preparedness.

The DHS Organizational Element Chief Information Officer will:

Manage acquisition, use, and disposition of telecommunications resources (services, facilities, and equipment);

Establish policy and procedures for the management and cost control of telecommunications systems, subject to guidance from the DHS CIO;

Provide advice and assistance to offices regarding telecommunications services and facilities;

Serve as liaison for telecommunications related activities and interchange between the Operating Unit and Department of Homeland Security;

Ensure that the telecommunications services, including the Government-provided long distance network, are used for official Government business and authorized purposes by authorized personnel;

Ensure that the appropriate level of telecommunications service is furnished each employee;

Establish appropriate limitations and controls over the acquisition, use and disposition of telecommunications resources;

Establish an appropriate usage oversight program sufficient to manage telecommunications costs; and

Manage, review, and verify telecommunications billing to ensure that telecommunications services and equipment are billed and paid in accordance with established standards of practice. Monitor invoices and bills for waste, fraud, and abuse.

Billing and Accountability - Managing the cost of telecommunications:

Telecommunications Resources must be fiscally managed to ensure that the Government receives agreed-upon goods and services for money spent. Each operating unit must ensure that appropriate programmatic measures are in place to receive and evaluate billing or invoicing for telecommunications, determine its accuracy, and make timely and accurate payment.

Operating Units must establish and maintain management systems, which account for telecommunications resources, reconcile the billed costs for these resources with their use, and ensure that payment is accurately made. Offices must establish such systems and measures as are required to be in compliance with the laws, regulations, and procedures of the Federal Government and the Department of Homeland Security.

To effect these measures, operating units should, to the maximum extent possible, use automated processes, including the acquisition of billing detail in automated format and the use of automated systems to examine billing data for improper billing or usage. Operating unit managers should work closely with telecommunications vendors and the General Services Administration (Federal Technology Service) to obtain vendor participation and assistance in this effort.

Billing and accountability for wireless services should receive particular attention. At the time of this policy, these services are more expensive than terrestrial-based services and their costs may vary greatly depending on the vendor and usage "plan" selected. Operating unit managers should evaluate usage and billing data to determine the most cost-effective acquisition and usage "plan" for each user of wireless services.

Records Management and Access to Records:

Telecommunications usage and inventory records constitute systems of records, under the Federal Records Schedule (FRS), and must be managed, protected and disposed of in accordance with the FRS and the Department of Homeland Security Records Schedule. In addition, in compliance with the Freedom of Information Act (FOIA), telecommunications records must be made and maintained in such manner as to be accessible in response to established, determined and legitimate requests either from within the Federal Government or in response to requests under the FOIA.

The creation and retention of telecommunications records generally are performed in response to a need for the recorded information for purposes of managing telecommunications resources. Frequently, Call Detail Records (CDRs), for example, are created and retained to ensure appropriate sizing and facilitating of telecommunications systems. While specific types of records are not required under this policy, operating units must determine their records needs, given their management requirements. Once records are created, their retention and disposition are governed by the appropriate records schedules.

How do we ensure security of telecommunications resources?

As a subset of Information Technology, telecommunications resources and systems are subject to the same security considerations as other IT resources. The comprehensive DHS IT Security Policy is located on the IT Management Handbook under Security. Systems, services, and other resources must be offered a level of physical security that is appropriate to the application for which the resource is to be used. Since telecommunications resources, in most cases, utilize much the same technologies, it is necessary to provide physical security in the same ways as other IT resources. Since the applications for which telecommunications resources are applied are usually similar or complimentary, security should be applied to telecommunications resources based on the criteria applied to security of other IT resources.

As stated earlier, telecommunications, which either constitutes or is part of a system must be considered an Information Technology System, for all planning, acquisition, policy, security, and functional purposes. Telecommunications security must be assured in accordance with the DHS IT Security Policy. This policy requires that all IT Systems be certified and accredited in accordance with TBD of the policy.

Current technology already merges much of the telecommunications for voice and data over single resources. Soon, most or all telecommunications and networking may utilize a single transmission and connectivity technology, such as Voice or IP, or the like. Telecommunications, for the most part, cannot be seen or treated, as a unique resource having different security needs.

Consideration of security for telecommunications resources should always take into account the fact that telecommunications is an essential and critical resource for the function of the business of the Department of Homeland Security. Further the applications and transmissions over telecommunications resources must be understood to be essential and critical as well. Just as a data or PC-based network must have appropriate security, so a telecommunications network, which may often be the same network, must have equivalent security.

Password Security: Requirements for telecommunications resources password protection are the same as those for other IT resources, as outlined in DHS policy on use of passwords. An exception is made for telecommunications devices and resources that have no capability for password protection, such as standard voice termination units (telephones). An exception is also made for those devices or resources that have different, limited capabilities, such as the capability for only limited password protection or shortened passwords.

National Security and Emergency Preparedness: There are numerous aspects of telecommunications, which fall under this heading within the Department of Homeland Security. These include:

Communications Security (COMSEC) (STU III / STE)

National Communications System (NCS) participation

Telecommunications Service Priority (TSP)
Government Emergency Telecommunications Services (GETS)

Red Switch Phone services

May telecommunications transmissions or conversations be recorded or monitored?

At times, in the conduct of business within call center functions, there is a need to record or monitor voice transmissions or conversations for management purposes. This may be done only under very limited circumstances and only with the approval of both the Operating Unit CIO and the DHS CIO. The following circumstances must be present in order to permit such monitoring to take place:

Both parties to a conversation must be aware of the recording or monitoring of a conversation or transmission.

In a call center environment, the caller must be notified that monitoring or recording will be performed. Notification must be made prior to initiation of the conversation itself, and may be accomplished by presenting a notice saying "This conversation (or call or transaction) may be recorded (or monitored) for training (or supervision or other reason) purposes. Please notify the agent if you wish this conversation not to be recorded."

If a caller does not want the call recorded, provision must be made to ensure that the recording capability is disabled during the call.

Prior to establishing a system that will record or monitor conversations or transmissions, a request must be made to the DHS CIO, stating the need, and approval must be received from the DHS CIO.

What is the final disposition of Telecommunications Resources?

Telecommunications physical resources (hardware, etc.) must be disposed of in accordance with the Department of Homeland Security Personal Property Management Manual, which is available through the Personal Property Division. The Personal Property Procedures Manual outlines the procedures, which are to followed when disposing of telecommunications equipment.

In addition, information on the full range of Federal property management may be found in the Federal Property Management Regulations: 41 CFR, C 101.

Who can address questions regarding this policy?

Contact: The Office of the CIO.

Where can I get additional information?

Additional information and guidance may be obtained from the Office of Chief Information Officer.

Additional Attachments & References:

Attachment B: Department of Homeland Security Nomination and Designation of Designated Agency Representative (DAR) For Telecommunications Services

Attachment C: Designated Agency Representative (DAR) for Telecommunications Services. Function Requirements

Reference: Title 41, Code of Federal Regulations; Chapter 101–Federal Property Management Regulations; Part 101-35 Telecommunications Management Policy (Federal Government)

Department of Homeland Security
Nomination and Designation of Designated Agency Representative (DAR)
For Telecommunications Services

This is a request for designation of the named employee as a Designated Agency Representative (DAR) for the specified operating unit(s) within the U.S. Department of Homeland Security for purposes of ordering telecommunications services from approved sources only. Limitations of authority for ordering are specified both on this form and in the Federal Acquisition Regulations and the Department of Homeland Security Acquisition Regulations (DAM, Part 1, Chapter 1, Page 2). In some cases, a DAR may be designated to provide services for more than one operating unit or bureau.

When completed, this form should be forwarded to: Gloria Sullivan, Office of Telecommunications Management, U.S. Department of Homeland Security, TBD. E-Mail to: TBD or FAX: TBD

A. DAR's First Name M.I. Last Name **THIS ACTION IS:**
_____ _____ _____ **New Designation_XXX__**
DAR's Title **Status Change** _____
_____ **Delete** _____

B. DAR's Supervisor (if different from Authorizing Official)
First Name M.I. Last Name
_____ _____ _____
DAR's Supervisor's Title and Address
_____
DAR's Supervisor's Address
_____
_____

C. DAR's Organization Agency/Bur. Code
_____ _____

D. DAR's Phone Number _____ FAX Number _____
DHS/Bureau E-Mail Address Internet E-Mail Address (if different)
_____ _____
Mailing Address:
_____
Street
_____
City State Zip Code
_____ _____ _____

E. Organization(s) Represented by DAR
Organization Name Organization Code Organization Name Organization Code
_____/_____ _____/_____
_____/_____ _____/_____
DAR's Signature Date
_____ _____

Order Authority Level for which DAR is nominated: a. $25,000 __ b. $100,000 __ c. $500,000 __

Signature of Bureau Nominating Official Title Date
_____ _____ _____

Name of Bureau Nominating Official (Print) Title
_____ _____

- -

The nominee above is authorized as a Designated Agency Representative (DAR) with the authority to place orders with the value not to exceed that specified below.

DAR must meet the general qualification standards outlined in the Commerce Function Requirements DHS document. Nominee prior to designation must complete specific DAR training. In addition, within 3 months of initial designation, DAR must receive COTR training. Within 6 months of designation, DAR must complete a DHS-specified course in basic contracting. COTR or basic contracting courses completed within the past 2 years prior to designation may be substituted for this training at the discretion of the COTR.

Approved: Date Date
COTR C/O, Acquisition Services
_____ _____ _____ _____

DAR Training Date: _____ COTR Training Date: _____ Contracting Training Date: _____

TRAINING COURSES FOR DHS DAR PROGRAM:

Three training courses are required for each Designated Agency Representative (DAR). These are:

DAR Training;
COTR Training, and;
Simplified Acquisition.

The FTS2001 vendor, Sprint, provides DAR training. COTR training may be taken from many sources, but must be a 40-hour course. Simplified Acquisition may also be taken from many sources, but must include the following topics: Contract Administration, Past Performance, and Delivery Order Procedures.

The following course list shows some of the sources for the training. The cost for training courses is the responsibility of the Bureau or operating unit.

Designated Agency Representative (DAR)
For Telecommunications Services
Function Requirements

SCOPE AND DESCRIPTION OF DAR FUNCTION

The Department of Homeland Security awarded Delivery Order number TBD under the GSA FTS2001 Contract number GS00T99NRD2002 to Sprint for its department-wide telecommunications needs. The delivery order, awarded on an indefinite delivery / indefinite quantity basis, provides a simplified method of ordering telecommunications services. Individuals authorized to place service orders are referred to as Designated Agency Representatives (DARs).

A DAR must receive delegated procurement authority by the Director of Acquisition Services, Office of Acquisition Management in accordance with the Department's Contracting Officer Warrant Program which is contained in Part 1 of the Commerce Acquisition Manual (CAM). The Designated Agency Representative is responsible for reviewing and approving requests for services, as well as ordering, inspecting, and accepting services acquired under Delivery Order TBD The delegated authority may be amended to allow for ordering authority under other contractual vehicles, as may be deemed appropriate. Other possible service contracts may include the Metropolitan Area Access (MAA) contracts or the Washington Interagency Telecommunications Service (WITS).

Each DAR, though programmatically subject to normal chain of command within each operating unit, is subject to guidance and oversight from the COTR, ACOTR and Contracting Officer for purposes of acquisition. The DAR, the COTR and the ACOTR functions should become a stipulated performance element for each employee performing these functions. Except under unusual circumstances, the COTR and ACOTR have no responsibility for actually placing orders. The DAR is expected to play a meaningful role in the planning and development of requirements, providing primary liaison function with the FTS2001 vendor. In this role, the DAR may be involved in facilitating meaningful interaction with the vendor, including setting up meetings, exploring possible technical options, etc. Generally the DAR should be involved in the process prior to finalization of requirements. In all cases, the DAR is responsible for actual placement and management of orders.

A. POSITION GRADING AND TRAINING

No single, specific classification series or grade level is required for this position. All DARs, however, must have at least the level of qualifications outlined in this DHS document.
This function requires both specific and varied experience and training in the field of telecommunications and telecommunications management. It also requires the

following specific course work prior to receiving authorization to order services or to receiving a warrant for commitment of Government funds.

Designated Agency Training as provided by the General Services Administration (GSA) and by the Department of Homeland Security (DHS)

2. Contracting Officer's Technical Representative (COTR) Training
3. Basic Contracting

A DAR nominee prior to designation must complete specific DAR training. In addition, within 6 months of initial designation, a DAR must receive COTR training and within 12 months of designation, a DAR must complete a DHS-specified course in basic contracting. COTR or basic contracting courses completed within the 2 years prior to designation may be substituted for this training at the discretion of the COTR. The initial DAR designation, level A, carries a warrant sufficient to allow a DAR to acquire up to $25,000 of service per order. Upon completion of COTR training, the DAR may be granted a warrant of $100,000 per order and upon completion of Basic Contracting the DAR may be granted a warrant of $250,000 per order.

B. KNOWLEDGE, SKILLS AND QUALIFICATIONS REQUIRED BY THE FUNCTION

The Designated Agency Representative (DAR) is a function within Telecommunications Management and Acquisition. Typically a DAR is a technical specialist or analyst who works in a position that involves: 1) technical and analytical work in the planning, development, acquisition, testing, integration, installation, utilization, or modification of telecommunications systems, facilities, services, and procedures; 2) work in the planning, implementation, or program management of telecommunications programs, systems, and services; or, 3) functional responsibility for communications operations, planning or recommending changes.

DARs apply practical knowledge of commonly applied telecommunications and acquisition principles, concepts, and methodologies in performing review or analysis of telecommunications service requests, evaluating adequacy and appropriateness of requested services, consulting with requester, COTR or Contracting Officer, as needed, and with other appropriate persons. Work is generally independent involving both small and large projects, with responsibility for ordering, ensuring funding, tracking of order activity, ensuring timely provisioning and providing inventory management for services under specified contract(s).

DARs should have skill in weighing the impact of variables such as cost, variations in electronic and other equipment and service characteristics for compatibility or interoperability, equipment availability, and the kinds of communications required and available under the pertinent contract(s). DARs should have knowledge of standardized telecommunications equipment, services, and processes or established variations, allowing review of contractual relationships for equipment and services, network requirements, compatibility with established systems, optimization of services, security and other requirements.

For some DARs, this includes knowledge of operating characteristics and interoperability requirements for a variety of specialized communications systems such as office automation networks, satellite and video telecommunications, and digital networks.

DARs must also have a thorough basic understanding of acquisitions principles, requirements and regulation within the Federal government and within the Department of DHS. Because DARs function as ACOTRs, specific COTR and basic acquisitions training is required for this function.

C. GUIDELINES

Guidelines available and regularly used in the work are in the form of Federal Acquisition Regulations (FAR), Federal government telecommunications policy (resident within the FAR), agency policies and implementing directives, DHS Acquisition Manuals (DAM), handbooks, or locally developed supplements, as appropriate.

- -

REMAINING AREAS:

Communications Security (COMSEC)
DTS
DMS
ERLink (emergency response link)
GETS
NCC for Telecommunications
NS/EP
Overseas Secure Comm.
TSP
Red Link Phone
Comm. Center