



Government Facilities Sector-Specific Plan

An Annex to the NIPP 2013

2015



Homeland
Security

GSA

TABLE OF CONTENTS

GOVERNMENT FACILITIES SECTOR GOVERNMENT COORDINATING COUNCIL LETTER OF SUPPORT ii

EXECUTIVE SUMMARY 1

1. INTRODUCTION 4

2. SECTOR OVERVIEW 5

 2.1 Sector Profile 5

 2.2 Sector Risks..... 8

 2.3 Critical Infrastructure Partners..... 9

3. VISION, MISSION, GOALS, AND PRIORITIES..... 13

4. ACHIEVING SECTOR GOALS 16

 4.1 Risk Management..... 16

 4.2 Critical Infrastructure and National Preparedness..... 29

5. MEASURING EFFECTIVENESS..... 30

Appendix A Glossary of Terms..... 32

Appendix B List of Acronyms and Abbreviations..... 42

Appendix C Summary of Relevant Authorities 45

Appendix D Facility Components and Roles..... 47

Appendix E Coordination and Information Sharing Mechanisms 48

Appendix F SSA and GFS Program Support and Initiatives..... 52

Appendix G Continuity..... 61

Government Facilities Sector Government Coordinating Council Letter of Support

With the issuance of Presidential Policy Directive 21 (PPD-21), the connection between the security of critical infrastructure and its resilience was formalized, and a renewed national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure was initiated. PPD-21 designated the Department of Homeland Security (DHS) and the General Services Administration (GSA) to serve as co-leads for the Government Facilities Sector (GFS) and the Federal interface for the Sector. This responsibility is based on the foundation of expertise that each agency brings to this mission area.

Since 1949, when the GSA was established, its role as an owner/operator of Federally controlled facilities has provided unique insight into what is required to manage facilities in a secure and sustainable manner throughout their lifecycle. The Homeland Security Act of 2002 ("Act") established DHS, combining 22 related organizations into a single department. Under the Act, DHS and GSA share the responsibility for the protection of Federal facilities and grounds. The Federal Protective Service (FPS) is the law enforcement and security organization within DHS that executes this mission in coordination with GSA.

PPD-21 further designated that both the Education Facilities Subsector, which covers schools, institutions of higher education, and trade schools, with the Department of Education as the Sector-Specific Agency, and the National Monuments and Icons Sector, with the Department of the Interior as the Sector-Specific Agency, be included as part of the Government Facilities Sector.

This Sector-Specific Plan provides a strategy for Federal facility resilience, establishes priorities for enhancing security and resilience for Federal facilities, and defines overarching strategic goals, objectives, and actions while acknowledging challenges that exist. The Plan addresses the time frame from 2016 to 2019 and will be reassessed after four years. Through addressing several core capabilities over this four year period, Federal facility security and resilience can be further enhanced. Beyond the Federal facility community, the larger government facility landscape of State, local, tribal, and territorial (SLTT) entities will benefit from this Plan as beneficial results are transferred for broad application.



L. Eric Patterson

**Director
Federal Protective Service
Department of Homeland Security
Sector-Specific Agency**



Robert Carter

**Associate Administrator
Office of Mission Assurance
General Services Administration
Sector-Specific Agency**



Caitlin Durkovich

**Assistant Secretary
Office of Infrastructure Protection
U.S. Department of Homeland Security**

EXECUTIVE SUMMARY

The Government Facilities Sector (GFS) includes more than 900,000 constructed assets owned or operated by the Federal Government alone. The assets owned or operated by the 56 States and territories, 3,031 counties, 85,973 local governments, and 566 federally recognized tribal nations also fall in the purview of the GFS. In addition, the GFS comprises two subsectors: Education Facilities (EF) and National Monuments and Icons (NMI). Collectively this constitutes one of the largest and most complex sectors within the National Infrastructure Protection Plan 2013 (NIPP 2013) framework. PPD-21 identifies the General Services Administration (GSA) and the Federal Protective Service (FPS) as co-Sector-Specific Agencies (SSA) for the GFS.

Government Facilities Sector Assets and Risks

The GFS focuses on those threats and hazards that are likely to cause harm and employs prioritized approaches that are designed to prevent or mitigate the effects of incidents by following the risk management framework outlined in the NIPP 2013. This framework not only allows owners and operators to make risk-informed decisions that best allocate limited resources, but also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services during incidents and to support rapid response and restoration.

Risk Assessment

Many stakeholders conduct physical and cyber risk assessments using a broad range of methodologies to address their specific context and to meet their own decision-making needs. The challenge of minimizing the disparity in these approaches must be addressed through core risk assessment criteria and standards facilitated by teams of facility subject matter experts to ensure that essential mission functions will be carried out during emergencies. This process includes both the analytic principles that apply to all parts of a risk methodology and the specific guidance needed to understand and address each of the three components of the risk equation: consequence (C), vulnerability (V), and threat (T). Whenever possible, DHS seeks to use information from these particular assessments to better understand risks across all critical infrastructure sectors and regions throughout the Nation.

Cyber Risk Management

Cybersecurity risks and trends, when taken collectively, reach levels of scope and complexity that fall beyond the ability of individual industry and government organizations to manage. For example, when multiple organizations in an industry use the same software platform, they become vulnerable to the same exploits. While organizations typically manage these types of issues on an individual basis or with a few key partners, examining risks from a sector level can provide significant long-term benefits. Working together, organizations can play an active role in identifying shared risks or those that threaten the viability or sustainability of the industry's products, services, or functions.

Sector R&D

Numerous ongoing research and development (R&D) initiatives in both the public and private sectors have application to the GFS. Review of sector challenges, technology requirements, best practices, and current known R&D initiatives is conducted with sector partners representing the views of the sector.

Partnering to Improve Security and Resilience

The NIPP provides the framework for the cooperation that is needed to develop, implement, and maintain a national infrastructure security and resilience effort that brings together government at all levels, the private sector, and international organizations and allies. As co-SSAs, GSA and FPS are partners in collaboration with Federal, State, local, tribal, and territorial (SLTT), nongovernmental, and private sector entities. This Sector-Specific Plan (SSP) identifies and

presents the unique characteristics and risk landscape of the GFS, describes how the NIPP risk management framework is applied, and works to achieve shared goals and priorities to reduce critical infrastructure risk and enhance critical infrastructure security and resilience across the GFS.

2016 Sector-Specific Plan

This SSP aligns with the overarching vision, mission, goals, and priorities of the NIPP 2013 and requires coordination for protective activities across the sector. This document should be used by sector partners to provide guidance and focus on the development of physical and cyber security plans for the next four years.

In this SSP, sector goals are mapped to the NIPP 2013 goals and the Joint National Priorities (JNP), which were developed through cross-sector information sharing and collaborative working group sessions. They build upon an evaluation of emerging risks, known capability gaps, resource availability, and best practices. Together, the NIPP 2013 and JNP represent the community-wide distillation of the varied priorities pursued by individual government and industry entities. The JNPs are intended to focus partner efforts as they implement activities to accomplish the remaining NIPP 2013 calls to action, develop and implement updated SSPs, and pursue related efforts in furtherance of the NIPP 2013 strategic goals. Figure E1 is the map of GFS goals as it relates to the JNPs; however, it should be noted that the sector goals may not align exactly with the NIPP 2013 goals.

Figure E1: Sector Priorities mapped to the Joint National Priorities and aligned with the NIPP Goals

Government Facilities Sector Priorities	Joint National Priorities					NIPP Goals
	Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision Making	Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities	
A Progressively Implement a GFS Risk Management Program	PRIORITY A			PRIORITY A		Assess and analyze risks to critical infrastructure (T, V, C) to inform risk management activities.
B Organize and Partner for GFS Security and Resilience		PRIORITY B		PRIORITY B	PRIORITY B	Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery.
C Integrate GFS Security and Resilience as Part of the Homeland Security Mission	PRIORITY C		PRIORITY C	PRIORITY C	PRIORITY C	Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
D Manage and Develop the Capabilities of the GFS	PRIORITY D	PRIORITY D	PRIORITY D		PRIORITY D	Promote learning and adaptation during and after incidents and exercises.
E Maximize Efficient use of Recourses for GFS Security and Resilience		PRIORITY E	PRIORITY E		PRIORITY E	Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.

This SSP has several differences of note from previous SSPs: (1) SLTT partners now have access to the ISC standards; the ISC Risk Management Process (RMP) is available to the SLTT and may be an option for consideration, as adopting it would promote uniformity and helps the SSA measure progress across the Sector; (2) sector partners should report on their most critical assets, accomplishments, and challenges for the National Annual Report (NAR); (3) this SSP is focused to the operator level as opposed to the executive level; and (4) it includes cyber-specific protection efforts including:

- The NIST Cybersecurity Framework that focuses on using business drivers to guide cybersecurity activities and to consider cybersecurity risks as part of the organization's risk management processes.
- The C-Cubed Voluntary Program, which is focused on engagement with SSAs and organizations to develop guidance on how to implement the NIST Cybersecurity Framework.
- The Enhanced Cybersecurity Services program (ECS) is a voluntary information sharing program that assists U.S.-based public and private entities as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration.

The integration of cyber and physical security planning is consistent with Executive Order 13636 "Improving Critical Infrastructure Cybersecurity," which directs the Federal Government to coordinate with critical infrastructure owners and operators to improve information sharing and to collaboratively develop and implement risk-based approaches to cybersecurity. This effort also aligns with the National Preparedness System called for in Presidential Policy Directive 8 (PPD-8) in describing activities to manage risks across the five national preparedness mission areas of Prevention, Protection, Mitigation, Response, and Recovery.

Sector-Specific Goals

PPD-21 requires each SSA to provide the Secretary of Homeland Security with annual reports that serve as a primary tool for assessing performance and reporting progress toward sector goals. The NAR provides a platform for each sector to communicate protection performance, progress, and priorities to sector partners. This information is compiled by DHS and submitted to the President of the United States.

Progress toward achieving sector goals is assessed by measuring the performance of protective programs, assessment, and progress reporting. Such measures inform the risk management efforts of partners throughout the critical infrastructure community and help build a national picture of progress toward the vision of the NIPP. SSAs encourage partners to participate in data calls, working groups, GCC meetings, and other sector specific reporting mechanisms. The SSA will continue to share information with all stakeholders, identifying sector vulnerabilities, strategies, and best practices. This information will then be included in the NAR.

1 INTRODUCTION

The purpose of the 2016 Government Facilities (GFS) Sector-Specific Plan (SSP) is to help guide and integrate the Sector's continuous efforts to secure and strengthen the resilience of critical infrastructure over the next four years. It describes how the GFS contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21 (PPD-21), which directed the General Services Administration (GSA) to share the SSA responsibility to lead the GFS with the Federal Protective Service (FPS). PPD-21 also moved the National Monuments and Icons (NMI) Sector into the GFS, which already included the Education Facilities (EF) Subsector.

As an annex to the National Infrastructure Protection Plan 2013, "Partnering for Critical Infrastructure Security and Resilience" (NIPP 2013), this SSP follows the strategic guidance provided in NIPP 2013 and updates and augments prior versions of the SSP; it includes discussions of evolving risks and threats such as cyber and physical security, aging infrastructure, and collaborative efforts.

This SSP represents a collaborative effort among the private sector; State, local, tribal, and territorial (SLTT) governments; nongovernmental organizations; and Federal departments and agencies to work toward achieving shared goals and priorities to reduce critical infrastructure risk. It also reflects the maturation of the GFS partnerships and the progress made by the sector to address the evolving risk, operating, and policy environments since the 2010 SSP. New to this SSP is an effort to help standardize the assessment process by making the Interagency Security Committee (ISC) standards available to the SLTT, and to encourage participation in National Annual Reporting by sector partners in their effort to secure critical infrastructure and identify remaining challenges. Nothing in this SSP is intended to alter or impede the ability of any sector partner to perform their respective responsibilities under the law.

The SSP presents the unique characteristics and risk landscape of the GFS and describes how the NIPP 2013 risk management framework is applied. In addition, this SSP provides priorities for collaborative planning among Department of Homeland Security Office of Infrastructure Protection (IP) and the Government Coordinating Council (GCC). Partners have a clear and shared interest in ensuring the security and resilience of critical sector assets, systems, and networks, and this plan represents the voluntary, collaborative activities that could greatly reduce sector risk and build resilience during the next four years.

The remainder of this GFS SSP is organized as follows:

- **Chapter 2: Sector Overview**—Provides a view of the sector's assets and operating characteristics, risk profile, and key stakeholders.
- **Chapter 3: Vision, Mission, Goals, and Priorities**—Presents the sector's vision and mission, updated goals and priorities for security and resilience for the next four years, and the specific activities stakeholders plan to conduct.
- **Chapter 4: Achieving Sector Goals**—Describes the mechanisms to achieve sector goals, including ongoing and planned partnership programs, activities, and resources that support the sector's current risk management approach; research and development (R&D) priorities; and how the sector supports national preparedness through incident response and recovery.
- **Chapter 5: Measuring Effectiveness**—Describes the planned approach to measure the effectiveness of individual activities and report on sector progress.

2 SECTOR OVERVIEW

2.1 Sector Profile

Unlike the other sectors, the GFS is uniquely governmental; its facilities are either owned or leased by government entities. The importance of these facilities stems from the services they provide to the American people. Citizens interact with government on a daily basis, whether to obtain a driver’s license or apply for benefits or programs. Government facilities exist to facilitate the conduct of the Nation’s business. This section describes the characteristics of the GFS infrastructure, discusses overlaps with other sectors, and explains the existing regulatory environment.

Sector Facilities

Collectively this constitutes one of the largest and most complex sectors within the NIPP 2013 framework. The GFS includes a wide variety of facilities owned or leased by Federal, State, local, tribal, or territorial governments, located both domestically and overseas. Although some types of government facilities are exclusive to the GFS, government facilities also exist in most other sectors. Many government facilities are open to the public for business activities, commercial transactions, provision of services, or recreational activities. Other facilities not open to the public contain highly sensitive information, materials, processes, and equipment.


Government Facilities Sector Assets
900,000 constructed assets owned or operated by the Federal Government.
Assets owned or operated by:

- 56 States and Territories
- 3,031 Counties
- 85,973 Local Governments
- 566 Federally Recognized Tribal Nations

Education Facilities Subsector assets

Public Facilities

- Offices and office building complexes
- Housing for government employees
- Correctional facilities
- Embassies, consulates, and border facilities
- Education facilities
- Courthouses
- Maintenance and repair shops
- Libraries and archives
- Monuments



Non-Public Facilities

- Research and development facilities
- Military installations
- Record centers
- Space exploration facilities
- Storage facilities for weapons and ammunition, precious metals, currency, and special nuclear materials and waste
- Warehouses used to store property and equipment












The GFS has adopted an approach to categorize infrastructure that considers a facility’s predominant use rather than its ownership. This approach allows for maximum sharing of best practices for risk reduction to like facilities across all levels of government. In addition to the facilities themselves, the GFS considers elements associated with and often contained, or housed, within a facility. This includes cyber systems that contribute to the protection of sector assets (e.g., building automation systems, access control systems, and closed-circuit television systems). Also included, are individuals who perform essential functions or possess tactical, operational, or strategic knowledge.

Sector Boundaries and Overlap

The GFS exists at the intersection of multiple sectors. To profile the cross-sector relationships and dependencies that affect the overall vulnerability of the sector, as well as the vulnerability of dependent sectors, interdependencies must be analyzed. As this process matures, it will involve the collaboration of sector participants to define the physical, cyber, mission, and human dependencies, and to identify measures to enhance the protective posture of all sectors.

Because government facilities exist in the majority of critical infrastructure sectors, primary sector responsibility for facilities is based on its predominant use, as shown in Table 1. Although the government may own or lease a particular facility, that facility may fall within the area of responsibility of another sector.

Table 1. Facility Predominant Use by Sector

Predominant Use		Responsible Sector
	Offices and office building complexes	Commercial Facilities
	Retail stores within government facilities, government agencies within commercial facilities	
	Housing or community service facilities provided for public use	
	Food service establishments within government facilities	Agriculture and Food
	Health clinics and medical units within government facilities	Healthcare and Public Health
	Transportation-related government facilities*	Transportation Systems
	Nuclear reactors, materials, and waste located in government facilities**	Nuclear Reactors, Materials, and Waste
	Police, fire, and emergency services stations	Emergency Services
	Emergency operations, command, dispatch, and control centers	
	Public works facilities associated with:	
	Water or wastewater treatment	Water
	Power or natural gas Highway or road service or maintenance	Energy
	Telephone or Internet service	Communications, Information Technology
	Highway or road service or maintenance	Transportation Systems

* Except for space exploration and any that are part of military installations.

** Except for all U.S. Department of Energy (DOE) facilities involved with storage or use of special nuclear material and all U.S. Department of Defense (DoD) nuclear facilities and materials associated with defense programs.

Dependencies and Interdependencies

Government facilities are highly interconnected, both physically and through a variety of information and communications technologies. Identifying, understanding, and analyzing interdependencies and dependencies are subject to challenges because of the diversity and complexity of facilities. Interdependencies vary widely, and each has its own characteristics. There are four principal classes of interdependencies:







- **Physical:** Two facilities are physically interdependent if the state of each is dependent on the material output(s) of the other. A physical interdependency arises from a physical linkage between the inputs and outputs of two agents; a commodity produced or modified by one infrastructure or resource (an output) is required by another infrastructure for it to operate (an input).
- **Cyber:** A facility has cyber interdependency if its state depends on information transmitted through the information infrastructure. Cyber interdependencies connect infrastructure and resources to one another via electronic information links. The outputs of the information infrastructure are inputs to the other infrastructure, and information is the “commodity” passed between the infrastructure and resources.




- **Geographic:** Facilities are geographically interdependent if a local event can change the state of all other facilities. This interdependency occurs when elements of multiple infrastructures are in close proximity.
- **Logical:** Two facilities are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection. Logical interdependencies link an agent in one infrastructure or resource to another without any direct physical, cyber, or geographic connection.

A dependency is a linkage or connection between two infrastructure sectors, through which the state of one infrastructure influences or is correlated to the state of the other. For example, under normal operating conditions, a government facility requires electricity, natural gas, and water to function. It requires information technology and telecommunications to carry out necessary operations, as well as road and rail transportation to move employees to and from the site to continue essential functions. The GFS illustrates the high-level dependencies that are operating within each sector.

The GFS is tightly integrated with other critical sector operations, which creates interdependencies that could cause a disruption in one sector or impact to safe operations in another.

Table 2: GFS Dependencies and Interdependencies

Sector	Dependency or Interdependency
	Provides power, which supports critical facility functions, such as lighting, water pumping, and HVAC systems. This is the primary dependency for the GFS. Without power, many facilities could not function for an extended period of time, as access to backup power is often limited in scope. An interruption to the power supply would directly affect all facilities located in the region serviced and could have cascading effects on other sectors.
	Provides a supply of potable water for and handles the treatment of wastewater. The sector also provides water for fire suppression systems. Without these services, government facilities might need to be shut down until services are restored.
	Saves lives and protects property after incidents, such as accidents, natural disasters, or terrorist attacks. The GFS coordinates with Emergency Services—which includes law enforcement, fire and emergency services, and emergency medical services—to mitigate risk and respond to incidents. A disruption would affect the GFS disaster response and prevention capabilities. Emergency Services also manages crisis re-entry for affected areas, which is a critical issue for GFS owners and operators trying to gain access to their facilities.
	Provides telecommunications access and enables operations. Damage to the Communications Sector would affect the ability of the GFS to operate and could cause cascading economic damages as employees and customers may have difficulty communicating. Disruption to critical communications operations in facilities, such as information networks or operation and dispatch centers, would hamper the sector's ability to respond and mitigate incidents.
	Provides the transportation of goods to and from government facilities, as well as the transportation of employees and visitors during regular operations and after disasters. A disruption in the Transportation Sector could prevent employees and visitors from reaching government facilities or keep them from being able to leave facilities after an incident. A disruption could also keep goods and supplies from leaving or reaching the GFS. The sector also needs to be able to gain access to areas after disasters to reconstitute services and reopen facilities.
	Enables day-to-day operations and financial transactions. Loss of function would affect the sector's ability to operate both cyber and physical systems.

Sector	Dependency or Interdependency
	Provides services to the public in the event of an attack, natural disaster, or pandemic/large-scale outbreak of an illness. Pandemics can spread easily through government facilities, as large groups of people congregate daily.
	Provides essential services for the GFS to conduct daily business operations and emergency response. During disasters, government facilities may house ATM and banking resources that the public will need to access during incidents.
	Resides within or adjacent to GFS facilities as tenants or government offices reside within commercial facilities. This creates a shared risk environment to both sectors, which promotes collaboration to address security challenges.

Key Authorities

The primary authority for critical infrastructure security and resilience efforts is PPD-21¹ which specifies responsibilities for Federal departments and agencies, as well as State, local, tribal, and territorial government sector partners. Numerous authorities apply to aspects of government facility protection. Although some are broadly applicable to all levels of government, others are specific to a particular government entity or single facility type. In some cases, specific authorities may only be applicable to portions of a particular facility. For example, Federal regulations apply to Federally owned or leased buildings. However, if only a portion of a building is leased by a Federal entity, only the area under Federal control or authority is subject to Federal regulations.

Authorities cover both cyber and physical security. Federal laws, regulations, and standards require all Federal organizations to establish effective security assessment processes for information technology (IT) that provides assurance that risks associated with IT systems are properly understood and secured, documented, and accepted throughout the lifecycle of the system.

As such, authorities must be carefully examined to ensure that applicable requirements are being met for each government occupied facility. Appendix C includes an overview of GFS authorities.

2.2 Sector Risks

Government facilities represent attractive and strategically important targets for both domestic and international terrorist groups as well as criminals. These assets are often targeted because they provide unique services, perform sensitive functions, contain irreplaceable artifacts, or have significant symbolic value. To minimize vulnerability, sector partners incorporate the risk management framework. Due to the size and high profile nature of the sector, government facilities function within a dynamic threat environment requiring a constant flow of reliable information regarding active threats. In addition, due to the openness of government facilities that are personnel-centric, service-oriented, or serve as monuments and museums, the public is an important factor in determining the appropriate facility protection. Numbers of visitors to a facility may vary widely due to time of day or seasonal factors, and the facility protective posture should change accordingly.






Natural and manmade events are the two major sources of risk to the GFS. Successful risk management involves examining the applicability of the various threat sources to a facility and its associated assets through an analysis of historical and quantitative data on threats, hazards, and actual incidents, as well as real-time situational awareness.

¹ Presidential Policy Directive 21, (PPD-21) updated the requirements for the development of the NIPP.

However, cybersecurity risks and trends, when taken collectively, reach levels of scope and complexity that fall beyond the ability of individual industry and government organizations to manage. For example, when multiple organizations in an industry use the same software platform, they become vulnerable to the same exploits. While organizations typically manage these types of issues on an individual basis or with a few key partners, examining risks from a sector level can provide significant long-term benefits. Working together, organizations can play an active role in identifying shared risks or those that threaten the viability or sustainability of the industry’s products, services, or functions.

Table 3 lists the broad range of common threats that are typical to the GFS.

Table 3: Range of Threats

	<p>Natural threats include those that are meteorological, geological, or biological and are typically present in defined geographic areas. Increasingly severe weather events can cause significant property damage, threaten the safety of employees and visitors, and limit access to critical resources such as power, water, transportation, and food supplies. Specific natural threats that can affect government facilities around the world should be identified according to likelihood of occurrence. Extreme space weather can cause disruptions of critical services such as interruption of power causing cascading effects on all services. Examples of natural threats include severe storms, hurricanes, earthquakes, tornadoes, volcanoes, drought, floods, landslides, tsunamis, wildfires, climate change, and coronal mass ejection/space weather.</p>
	<p>Manmade threats are divided into two categories: intentional and unintentional.</p> <p>Unintentional threats are caused by human errors and omissions (accidental); or an equipment failure (technological). Examples include carelessness, failure to understand policy, social engineering, security violations, coercion, and manipulation.</p> <p>Intentional threats are categorized based on the intent of the potential aggressor. These attacks are infrequent in nature; consequently, there is no standardized dataset that can provide probability information for terrorism. However, based on research by various experts, certain facility characteristics suggest how attractive a facility may be to a terrorist, thus providing a proxy for relative probability. Examples include, but are not limited to, terrorist acts; criminal act/ malicious behavior; active shooter; assassination; chemical, biological, radiological, nuclear, and explosive event (CBRNE); hostage-taking; cyberattacks; denial of services; hacking; malicious software and code; insider threat; public unrest; supply chain disruptions; and drone/aerial incursions.</p>
	<p>Pandemics occur when an infectious agent emerges against which humans have little immunity. Influenza viruses are very diverse and have the propensity to mutate, which complicates the development of adequate vaccines and antiviral medications. A pandemic could severely threaten the large workforce of the sector, compromising facility operations or limiting services. Pandemics can also spread easily through facilities as large groups of people congregate in them daily. These events could severely threaten facility operations, affecting delivery of essential functions and services and to the public. Types of events include pandemic and mass psychogenic illness, which occurs when social trauma or anxiety combines with a suspicious event to produce psychosomatic symptoms.</p>
	<p>Aging infrastructure can significantly increase vulnerabilities caused by natural and/or manmade events. It could also cause cascading effects, disruptions of services and/or delivery of critical mitigation and recovery equipment, and a greater physiological impact on the American people.</p>
	<p>Cyber threats are any circumstance or event with the potential to adversely affect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system. This can occur via unauthorized access, destruction, disclosure, modification of information, or denial of service. Cyber threat sources include corrupt employees, criminal groups, hackers, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary or political gain or mischief, among other things. Cyber threat sources may make use of various cyber techniques, or exploits, to adversely affect systems or networks.</p> <p>Federal facilities contain building and access control systems—computers that monitor and control building operations such as elevators, electrical power, heating, ventilation, and air conditioning—that are increasingly being connected to other information systems and the Internet. The increased connectivity heightens their vulnerability to cyberattacks, which could compromise security measures, hamper agencies’ ability to carry out their missions, or cause physical harm to the facilities or their occupants. Perhaps most importantly, a cyberattack could render these systems unavailable, leading to system outages that could result in the loss of ability to control temperature, physical access, lighting, or even life-safety systems.</p>

2.3 Critical Infrastructure Partners

GFS partners share in the responsibility for protecting government facilities with the understanding that they operate under varied authorities. The following sections describe broad sector partner responsibilities, as well as other responsibilities that are specific to Federal departments and agencies.

Sector-Specific Agency

PPD-21 identifies GSA and FPS as the co-SSAs for the GFS. In addition, the GFS includes two subsectors: the Educational Facilities (EF) Subsector and National Monuments and Icons (NMI) Subsector.



The **General Services Administration (GSA)** is an independent agency of the United States government established in 1949 to help manage and support the basic functioning of Federal agencies. The GSA supplies products and communications for U.S. government offices, provides transportation and office space to Federal employees, and develops government-wide cost-minimizing policies and other management tasks.

GSA's business lines include the Federal Acquisition Service (FAS) and the Public Buildings Service (PBS). Other divisions include the Office of Government-wide Policy, the Office of Mission Assurance, the Office of Small Business Utilization, and the Office of Citizen Services and Innovative Technologies. The official U.S. government web portal, USA.gov, and the Spanish-language web portal to U.S. government services, GobiernoUSA.gov, are members of the Office of Citizen Services and Communication's family of websites, which also includes pueblo.gsa.gov (the Federal Citizen Information Center), Kids.gov, ConsumerAction.gov, and WebContent.gov.



The **Federal Protective Service (FPS)** protects Federal facilities, their occupants, and visitors by providing law enforcement and protective security services, leveraging its access to the intelligence and information resources of its network of Federal, state, local, tribal, territorial, and private sector partners. From its frontline law enforcement and security personnel, to those who support the operations of the Service, FPS approaches its mission as one team. FPS conducts Facility Security Assessments (FSA) at over 8,700 FPS-protected GSA facilities nationwide. The FSA is the process and final product documenting an evaluation of the security-related risks to a facility. The FSA is

designed to identify Federal facility security risks and vulnerabilities and to offer tenant agencies solutions that will allow them to mitigate the impact of any undesirable event, from terrorist attacks to natural disasters. Every day FPS protects the homeland by managing risk and ensuring continuity for one of the most crucial elements of our national critical infrastructure—the people and the Nation's Federal facilities.

Subsectors



The U.S. Department of Education (ED) Office of Safe and Drug Free Schools serves as the SSA for the Education Facilities (EF) Subsector, and the Department of the Interior serves as the SSA for the National Monuments and Icons (NMI) Subsector. The Education Facilities Subsector includes facilities that are owned by both government and private sector entities, and covers pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools. The National Monuments and Icons Subsector encompasses a diverse array of assets located throughout the United States. Many NMI assets are listed in either the National Register of Historic Places or the List of National Historic Landmarks.

Government Facilities Sector Government Coordinating Council

The GFS Government Coordinating Council (GCC) enables interagency and cross-sector coordination. The GCC is comprised of representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of the sector.

The GCC is co-chaired by FPS and GSA as the designated Sector-Specific Agencies with the responsibility for ensuring appropriate representation on the GCC, providing cross-sector coordination with State, local, tribal, and territorial governments. The GCC is also co-chaired by the Department's Assistant Secretary for Infrastructure Protection or his/her designee. The Government Coordinating Council coordinates strategy, activity, policy, and communication across governmental entities within the sector. The primary functions of the GCC are to:

- Provide interagency strategic communications and coordination at the sector-level through partnership with DHS and other supporting agencies across various levels of government;
- Participate in planning efforts related to the development, implementation, update, and revision of the NIPP and development of the GFS SSP; and
- Coordinate strategic communications and resolution of issues amongst government entities within the sector.

Sector Partner Responsibilities

To support the implementation of the NIPP 2013 risk management framework within the sector, the following responsibilities are broadly applicable to all GFS partners:

- Coordinate efforts to enhance protection of government facilities;
- Establish goals and objectives for facility protection that support the NIPP 2013, JNP, and this SSP;
- Identify existing or establish and maintain inventories of government facilities, systems, and networks;
- Conduct risk assessments for high-consequence government facilities using an assessment methodology that meets the NIPP 2013 core criteria;
- Prioritize resource allocation to support protective programs that mitigate risks to facilities;
- Promote the coordination of protective and emergency response activities, preparedness programs, and continuity of operations/services, and identify resources for them;
- Facilitate the exchange of information, including threat assessments, attack indications, warnings, and advisories, for those having a need-to-know within and across government entities;
- Identify and communicate requirements for government facility-related R&D to the U.S. Department of Homeland Security (DHS);
- Participate in awareness and training programs to encourage appropriate management, protection, and overall preparedness of government facilities; and
- Annually provide information to the SSA on critical infrastructure facilities successfully addressing accomplishments and challenges in meeting the NIPP 2013 goals for inclusion in the GFS National Annual Report (NAR) to DHS.

State, Local, Tribal, and Territorial Governments Partner Responsibilities

SLTT government partners have unique responsibilities, functionalities, or expertise based on existing authorities and associated roles for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities and industries within their jurisdictions, including mutual aid agreements and communication plans where feasible and appropriate. These responsibilities are fulfilled through development and implementation of State Homeland Security (SHS) strategies. Critical infrastructure security and resilience programs should support the SHS strategies and reference all core elements of the NIPP 2013 framework, including key cross-sector

security and information-sharing linkages, as well as specific critical infrastructure security and resilience programs focused on risk management.

The SLTT Government Coordinating Council (SLTTGCC) is fully represented across all sectors and has established a liaison for each sector. The liaisons regularly participate in GFS GCC information sharing activities and meetings, and report on discussions and deliverables to the SLTTGCC. They also provide input from the SLTTGCC to the GFS GCC, ensuring the fullest possible representation of State and local perspectives.

The SSA promotes relationships between local law enforcement personnel and Federal departments and agencies (e.g., U.S. Secret Service, Federal Bureau of Investigation, and U.S. Capitol Police) to enhance situational awareness and information exchange. When appropriate, FPS and GSA participate in emergency-related exercises with State and local first responders.

Federal Partner Responsibilities

Some Federal departments and agencies also have unique roles and responsibilities as outlined in Table 4.

Table 4: Federal Roles and Responsibilities

Federal Entity	Roles and Responsibilities
U.S. Department of Commerce	Protection of National Weather Service facilities
U.S. Department of Defense	Protection of military installations and U.S. embassies and consulates
U.S. Department of Education	Coordination with Federal and non-Federal sector partners to help address risk management for schools
U.S. Department of Energy	Protection of facilities containing special nuclear materials
U.S. Department of Homeland Security – Federal Protective Service	Protection of Federal Facilities
U.S. Department of Justice	Protection of Federal courthouses through the U.S. Marshals Service
U.S. Department of State	Protection of U.S. embassies, consulates, and dignitaries
General Services Administration	Management of Federally owned and leased facilities
National Aeronautics and Space Administration	Protection of facilities associated with space exploration
National Archives and Records Administration	Protection of national archives, records, and artifacts
Federal Emergency Management Agency	Coordination of the National Continuity Program
U.S. Department of the Interior	General coordination of the National Monuments and Icons Subsector, as well as State and local monuments

The Department of Homeland Security

The Department of Homeland Security has an overall mission to reduce the Nation’s vulnerability to terrorist attacks, major disasters, and other emergencies. Many DHS components have overarching responsibilities associated with preparedness, coordination, and research and technology. The following are highlighted as examples of components particularly relevant to the Sector:

- **National Protection Programs Directorate (NPPD)** leads the national effort to protect and enhance the resilience of the Nation’s physical and cyber infrastructure.
- **The Federal Protective Service (FPS)** is responsible for the protection of federal facilities, their occupants, and visitors by providing law enforcement and protective security services.
- **The Office of Infrastructure Protection (IP)** is responsible for the implementation of the NIPP and conducts national-level infrastructure protection coordination and assessment activities.

- **The Office of Cyber and Infrastructure Analysis (OCIA)** conducts integrated threat analysis for all sectors to ensure a complete and sophisticated understanding of the cyber risks to the Nation’s critical infrastructure.
- **The Office of Cybersecurity and Communications (CS&C)** contains the Stakeholder Engagement and Cyber Infrastructure Resilience Division and the Office of Emergency Communications, which work cooperatively to secure and ensure the availability of the Nation’s cyber and telecommunications infrastructure.
- **The Office of Grants and Training** is responsible for assisting State, local, tribal, and territorial jurisdictions and regional authorities as they prevent, deter, and respond to terrorist acts.
- **The Science and Technology Directorate (S&T)**, the primary R&D arm of DHS, organizes the vast scientific and technological resources of the Nation to prevent or mitigate the effects of catastrophic terrorism and natural hazards.

3 VISION, MISSION, GOALS, AND PRIORITIES

This SSP aligns with the overarching vision, mission, goals, and priorities of the NIPP 2013 and requires coordination for protective activities across the sector. To accomplish the sector vision, mission, goals, and objectives have been established to provide a framework for sector activities that increase the protective posture of government facilities. These activities can allow for more standardized risk management throughout the GFS and produce tangible benefits for many sector partners. Beyond provisions for ensuring the protection of vital government assets, providing for national security, and supporting the continuity of the constitutional form of government, sector partners throughout the GFS can gain tangible benefits from meeting the objectives of the SSP. This document can be used by sector partners to develop security plans and provides focus for the next four years.

GOVERNMENT FACILITIES SECTOR VISION

Ensure the protection, safety, and security of government assets, employees, and visitors to facilities, as well as balanced management of physical and cyber risk, so that essential government functions and services are preserved without disruption.

GOVERNMENT FACILITIES SECTOR MISSION

The Government Facilities Sector will reduce the vulnerability to terrorist attacks, major disasters, and other emergencies that would affect domestically and internationally owned or leased facilities of the Federal, State, local, tribal, and territorial government entities; thereby facilitating and supporting the resilience and continuity of the Nation's operations.

Table 5: GFS Goals and Objectives

Goals		Objectives	
1	Progressively Implement a Government Facility Risk Management Program	1.1	Identify and obtain data for domestic and overseas facilities.
		1.2	Coordinate, facilitate, support and maintain comprehensive risk assessment programs that address domestic and overseas facilities.
		1.3	Identify, develop, promote, and maintain effective protective measures, programs, strategies, and related guidance for domestic and overseas facilities.
		1.4	Implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework to apply the principles and effective practices of risk management to improve the cyber and physical security and resilience of critical infrastructure or the attempt to map existing requirements, such as FISMA or Federal Information Protection Standard (FIPS) (thus calling on the NIST 800 SP series), back to the NIST Framework.
		1.5	Monitor performance to support continuous improvement and identify gaps and report progress to DHS via the NAR.
		1.6	Develop best practices and guidance for countermeasures for current threats to domestic and overseas facilities.
2	Organize and Partner for Government Facility Protection and Resilience	2.1	Understand and share information about intentional threats and unintentional hazards to domestic and overseas facilities.
		2.2	Build sector partnerships to share information about threats and hazards by implementing appropriate protection and resilience programs.
		2.3	Support continuity programs to ensure the protection of operations and government in the event of an attack or natural hazard.
		2.4	Share lessons learned and best practices as result of hot washes and after-action reports.

Goals		Objectives
3	Integrate Government Facility Protection as part of the Homeland Security Mission	3.1 Develop, review, and revise/maintain plans for critical infrastructure security and resilience to reinforce linkage between NIPP steady-state critical infrastructure security and resilience and National Response Framework (NRF) incident management requirements.
		3.2 Identify, review, revise, and implement plans and processes for enhancements of protective measures for all-hazard conditions in alignment with the National Threat Advisory System (NTAS) and the Continuity of Government Condition (COGCON) Threat Level Matrix. Follow sector-specific warnings communicated through the NIPP information-sharing framework, to include the Homeland Security Information Network (HSIN).
		3.3 Implement and support roles and responsibilities as defined in the NRF for incident management activities.
4	Manage and Develop the Capabilities of the Government Facilities Sector	4.1 Promote awareness, education, training, and exercise programs to increase understanding of risk to government facilities.
		4.2 Improve critical infrastructure cyber and physical security and resilience by advancing research and development solutions.
		4.3 Develop and maintain an SSP that supports the overarching NIPP goals and objectives.
		4.4 Promote the NIST Cybersecurity Framework, C-Cubed, and Enhanced Cybersecurity Services across the sector.
5	Maximize Efficient Use of Resources for Government Facility Protection	5.1 Determine sector priorities, program requirements, and funding needs for government facility protection.
		5.2 Enable or augment protection for those government facilities that are determined to be nationally critical and coordinate the efforts of sector partners and the use of resources from different funding sources.
		5.3 Outline which countermeasures are unfunded and develop mitigation strategies, to include analyses of alternatives.

Sector Priorities

Priorities are based on individual facility mission(s) needs and alignment to the NIPP 2013 and JNPs. Priorities should be realigned or adjusted due to the evolving threat and risk landscape and available resources. Goals above are listed in priority order. The sector is well focused at the Federal level as it is governed by PPD-8, PPD-21, and EO 13636.

Table 6: GFS Priorities

Goals	Priorities
1 Strengthen the management of cyber and physical risks to critical infrastructure	PRIORITY A₁ Promote the implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework to apply the principles and effective practices of risk management to improve the cyber and physical security and resilience of critical infrastructure and/or the attempt to map existing requirements, such as FISMA or FIPS (thus calling on the NIST 800 SP series), back to the NIST Framework.
	PRIORITY A₂ Educate critical infrastructure owners and operators within the GFS about cyber risk management, the Framework, and resources available through the C-Cubed program and recommend activities in order to strengthen cybersecurity within the sector.
2 Build capabilities and coordination for enhanced incident	PRIORITY B₁ Promote the coordination of protective and emergency response activities, preparedness programs, and continuity of operations/services, and identify resources for them.

Goals

Priorities

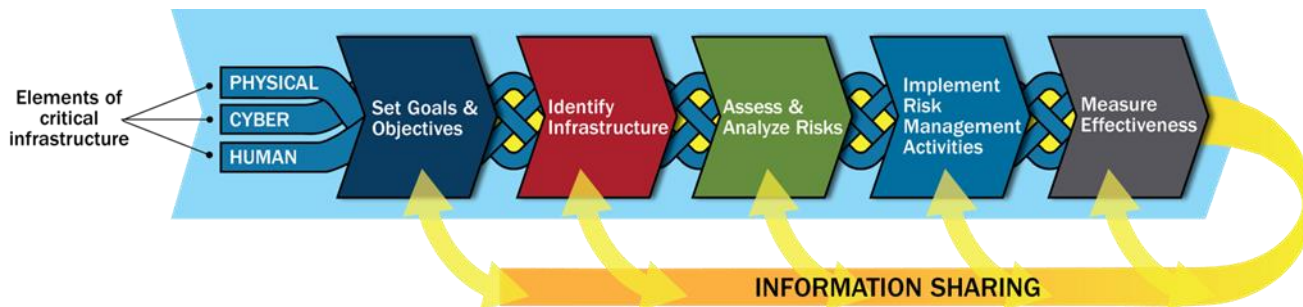
response and recovery	<p>PRIORITY B₂ Facilitate the exchange of information—including threat assessments, attack indications and warnings, and advisories—for those having a need-to-know within and across government entities.</p>
3 Strengthen collaboration across sectors, jurisdictions, and disciplines	<p>PRIORITY C₁ Evaluate emerging risks, known capability gaps, resource availability, and best practices. Share these findings.</p>
4 Ensure effectiveness in resilience decision making	<p>PRIORITY D₁ The GFS will continue to enhance information sharing through joint cyber and physical assessments by promoting the use of an evaluation team approach, consisting of representatives from the CSO, CIO, building management, engineers, and support services contractors. Senior management can use the information derived from consolidated risk assessments to make better risk-informed decisions and apply limited resources more effectively.</p>
	<p>PRIORITY D₂ Regular review of progress allows the sector to quantify the benefits achieved by specific activities, incorporate improvements into protective programs where needed, and inform future resource allocation decisions that focus on highest priority facilities via analysis and modeling to identify interdependencies and cascading effects.</p>
5 Share information to improve prevention, protection, mitigation, response, and recovery activities	<p>PRIORITY E₁ Information sharing is an essential component of the risk management process prescribed by the SSP. A trusted information-sharing network provides sector partners with the means to identify emerging threats and develop innovative protective programs and expertise, all necessary for the protection of government facilities. As the community of sector partners grows, additional information and expertise will be available, and a more comprehensive picture of GFS operations can be developed.</p>
	<p>PRIORITY E₂ The GFS uses coordination mechanisms to facilitate sharing of near-real time information on threats, vulnerabilities, incidents, recommended protective measures, and critical infrastructure security and resilience best practices.</p>
	<p>PRIORITY E₃ Share lessons learned and best practices as results of hot washes and after-action reports.</p>

4 ACHIEVING SECTOR GOALS

4.1 Risk Management

The GFS focuses on those threats and hazards that are likely to cause harm and employs prioritized approaches that are designed to prevent or mitigate the effects of incidents by following the risk management framework outlined in NIPP 2013. This framework allows owners and operators to make risk-informed decisions that best allocate limited resources. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services during incidents and support rapid response and restoration.

Figure 1: NIPP Risk Management Framework



Identify Infrastructure

Identify the components of the sector that, if damaged, would result in significant consequences, negative impact on national economic security, national public health and safety, public confidence, national governance, or some combination of these adverse outcomes. Items or materials contained within, or associated with, a government facility that may be exploited or damaged and require protection due to their unique or specialized characteristics include:

- **Facilities:** specialized or critical functions;
- **Equipment:** unique security devices, parts, or pieces of equipment;
- **Conveyances:** aircraft, spacecraft, or ground transportation vehicles housed within a government facility;
- **Records:** documents in digital or physical format;
- **Artifacts:** items of historic or iconic importance; and
- **Materials:** raw materials, supplies, or finished products such as chemical, biological, or radiological materials; explosives and ammunition; currency; and precious metals.

In addition, functions that support the government's ability to continue providing vital services, exercise civil authority, maintain the safety of the general public, and sustain the industrial/economic base are considered essential. The GFS categorizes essential functions based on the structure established by Homeland Security Presidential Directive 20 (HSPD-20) as follows:

- **National Essential Functions (NEFs)** represent the subset of government functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through Continuity of Operations (COOP) and Continuity of Government (COG) capabilities.
- **Primary Mission Essential Functions (PMEFs)** are those government functions that must be performed in order to support or implement the performance of NEFs before, during, and in the aftermath of an emergency.

To ensure that essential government functions remain resilient, it is the policy of the United States to maintain a comprehensive and effective continuity capability composed of COOP and COG programs to ensure the preservation of the American form of government under the Constitution and the continuing performance of NEFs under all conditions.

Cyber infrastructure includes cyber assets (e.g., hardware and software components), systems (e.g., a set of cyber assets that interact to perform a particular function), and networks (e.g., interconnected assets and systems that store, process, or communicate information), as well as the information contained in them. As building automation systems become more cyber reliant to improve operations and efficiency, they become more vulnerable to cyberattacks. Software is available that can monitor the network activity of computers running building control operations, such as elevators, electrical power, and HVAC systems, to establish a normal baseline of usage and notify building engineers when they detect unusual traffic on the network that could be an indicator of a cyberattack. Cyber infrastructure components may be identified individually or included as a facility cyber infrastructure, but fall within three primary categories:

- **Access control:** used to allow authorized personnel and visitors physical access only to defined areas of a facility;
- **Building Automated Systems:** used to monitor and control sensitive processes and physical functions; and
- **Warning and Alert:** used for alert and notification purposes to pass critical information that triggers protection and response actions.

Table 7: GFS Cyber Infrastructure Categories

Category	GFS Cyber Infrastructure			
	Asset	System (Major Application)	Network (General Support System)	Monitoring Technology and Information
Access Control	Card readers Badges Application software Databases	Interaction among the card reader, the badges, and the database	Communication of access control information within or between buildings	Access transactions Camera system data or live video feeds
Control	Chemical and food processing Electric distribution Water processing and control	Supervisory control and data acquisition Distributed control systems	Control local area network	Control commands Status information
Warning and Alert	Detection equipment Alarm systems	Telephone-based hazard alert systems Emergency alert system	Sensor network	Alerts Control commands Status information

The outcome of this process becomes part of the national inventory of information maintained by the U.S. Department of Homeland Security (DHS) to support steady-state critical infrastructure security and resilience and incident response. This data will be regularly verified and updated as sector partners report progress in meeting their goals during the National Annual Report data call collected by the SSA. This process will help focus resource allocation, influences effective design, implementation of protective programs and resilience strategies.

Assess and Analyze Risks

This section discusses several existing risk assessment methodologies and how the GFS applies the risk management process to ensure that the results of assessments are comparable throughout the GFS and with other sectors. The GFS is confronted with a wide variety of missions and facility types. As a result, a broad range of risk management strategies are applied. The risk management framework contributes to an understanding of risks across the sector and minimizes the disparity of risk assessment approaches.

Once identified, those assets should receive priority for a detailed risk assessment to provide reliable and comprehensive data to inform mitigation decisions, also recognizing dependencies and interdependencies are critical to the prioritization process. Many stakeholders conduct risk assessments to meet their own decision-making needs, using a broad range of methodologies. All assessment methodologies used by the GFS should meet the baseline criteria established in the NIPP. At the Federal level, assessment tools should be aligned and compliant with the Interagency Security Committee (ISC) Risk Management Process (RMP) to promote standardization across the sector. The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (Standard) defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level (FSL) and provides a single, integrated source of physical security countermeasures for all Federal facilities. The Standard also provides guidance for customization of the countermeasures for facilities.

The ISC offers a service to evaluate risk tools to determine whether they meet the NIPP criteria. The standards are now available through the ISC to SLTT facility security managers.

Whenever possible, DHS seeks to use information from stakeholders' assessments to contribute to an understanding of risks across sectors and regions throughout the Nation. To do this consistently, the challenge of minimizing the disparity in the approaches taken to conduct an assessment must be addressed through the core criteria identified below. These criteria include both the analytic principles that are broadly applicable to all parts of a risk methodology and specific guidance regarding the information needed to understand and address each of the three components of the risk equation: Threat (T), Vulnerability (V) and Consequence (C), to physical and cyber risk. The basic analytic principles ensure that risk assessments are:

- **Documented:** The methodology and the assessment must clearly document which information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. The types of decisions that the risk assessment is designed to support and the timeframe of the assessment (e.g., current conditions versus future operations) should be given.
- **Reproducible:** The methodology must produce comparable, repeatable results, even though assessments of different critical infrastructure will be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decision-makers.
- **Defensible:** The risk methodology must be technically sound, making appropriate use of the professional disciplines relevant to the analysis, as well as be free from significant errors or omissions. The uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates must be communicated.
- **Complete:** The methodology must assess consequence, vulnerability, and threat for every defined risk scenario and follow the more specific guidance for each of these as given below.

Risk assessments must provide reliable and comprehensive data so that sector partners can make informed decisions about which risk mitigation measures to implement. In some cases, sector partners design risk assessment processes, procedures, methodologies, or tools to meet the specific needs of the facilities they own and operate.

These factors are analyzed in a variety of ways throughout the GFS based on existing methodologies designed and implemented by sector partners. Risk assessments can be conducted at a variety of levels depending on the detail needed. For example, facility operators may conduct a very detailed and exhaustive risk assessment to determine all specific vulnerabilities of the facility in order to adopt certain countermeasures designed to enhance both cyber and physical security. Alternatively, an agency could evaluate risk across several similar facilities. Completion of an assessment is dependent on various factors, to include complexity, physical layout/size, mission, and interdependencies with other sectors.

Sector partners should maintain situational awareness regarding potential events that may impact and increase risk to their assets, system, and networks. As events occur, the risk for any individual facility may increase or decrease, and the prioritization and protection may change accordingly. The SSA works with sector partners at all levels of government to share information and coordinate enhanced protection strategies.

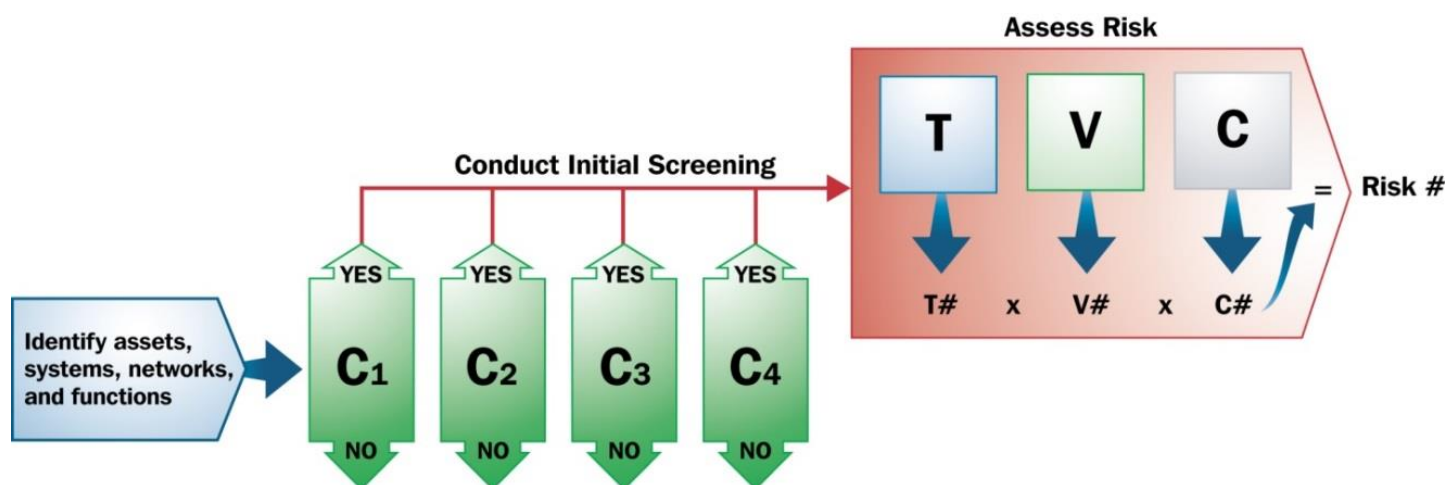
Risk assessments will increasingly involve mission dependency to fulfill continuity of operations and continuity of government compliance. In the process of defining and managing NEFs and PMEFs, risk management will increasingly focus on cyber-related dependencies and the vulnerabilities these create not only to the physical protection of government facilities, but also to the conduct of the missions housed within these facilities.

Consequence Screen

As an initial step in the overall risk assessment process, an infrastructure screening is performed to determine which GFS assets, if affected, could produce devastating impacts to governance, public health, the economy, or public morale and confidence. A set of criteria is provided to assist sector partners with this process. Facilities that pass through the consequence screen require a comprehensive risk assessment. At the most senior levels of government, certain positions receive individualized risk assessment and protection protocols; others are included as part of the facility assessment process. In addition, certain cyber systems are so critical to government operations that their presence in any individual facility must be considered in the risk assessment process and could significantly raise the overall risk to that facility. The three components of risk are evaluated and given a numeric value then combined to produce the overall risk rating.

Those assets or elements that could produce such results are determined to be critical and should receive priority for a comprehensive risk assessment.

Figure 2: GFS Process to Assess Risk



Assessing Threats

Threat is defined within the sector as the likelihood that the specific undesirable event will occur at an owned, operated, or leased government facility. Natural and manmade events are the two major sources of threats to the GFS. The threat assessment process involves examining the applicability of the various threat sources to a facility and its associated assets through an analysis of historical and quantitative data on threats, hazards, and actual incidents, as well as real-time situational awareness.

Information sharing and analysis of open source information can be used to draw conclusions about the threat environment. For example, many years of historical and quantitative data are available for natural hazards—along with probabilities associated with the cycle, duration, and magnitude of such hazards. This information provides a basis for assessing the threat to a facility. Criminal threats can be analyzed by using crime statistics compiled nationally as part of the Federal Bureau of Investigation’s (FBI) Uniform Crime Report or the National Crime Victimization Survey or through the use of crime statistics compiled by local law enforcement agencies. However, quantitative data that support analysis of

the broad range of terrorist threats remain scarce due to their infrequent and unpredictable nature. Because the magnitude and frequency of incidents and attacks vary widely and are difficult to predict, the determination of an intentional threat for any particular facility is difficult and largely subjective.

Although intelligence programs provide information on threats to facilities, it is vital for sector partners to maintain situational awareness of emerging threats because the GFS operates in such a dynamic threat environment. By sharing credible and accurate information in a real-time environment, sector partners can determine if additional protective measures may be needed to mitigate an imminent threat. However, sector partners should also consider whether any actions taken to mitigate a threat could cause secondary effects that would increase their overall threat level. For example, an unpopular regulatory decision or police action can incite protest and violence among segments of the population.

Assessing Vulnerabilities

Vulnerability is defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. Vulnerability encompasses two specific areas:

- Aspects of the facility itself that make it more or less likely that the selected threat would be successful; and
- Whether the countermeasure systems used at the facility are installed properly and functioning as designed.

Vulnerability is assessed based on the ability of the facility, its operations, and countermeasures to:

- **Deter:** Cause a potential attacker to perceive that the risk of failure is greater than the rewards associated with achieving success;
- **Detect:** Identify, classify, and validate potential threats;
- **Delay:** Lengthen the time a threat takes to cause its intended impact;
- **Deny:** Prevent a threat that is occurring from impacting the facility; and
- **Devalue:** Reduce the consequences of a threat that occurs.

Vulnerability assessments can be conducted at many different levels of detail and can focus on an individual facility, a campus of multi-agency facilities, a certain category of facilities, or the entire sector. Vulnerability assessments are designed to provide an in-depth analysis of the characteristics of the facility to identify weaknesses to determine corrective actions. The effect of interdependencies should also be considered to determine the extent to which it relies on and provides essential services for outside assets. Due to the interconnected nature of all critical infrastructure worldwide, the physical location of a government facility in the United States does not preclude international vulnerabilities as well as global dependencies and interdependencies.

A variety of vulnerability assessment methodologies are in use throughout the GFS. Some are available commercially, and others have been designed or adapted to meet the specific needs of a sector partner, facility, or campus of facilities.

When conducting vulnerability assessments, facilities are organized into zones and areas. This organization allows for a comprehensive assessment of the facility as it operates within the community where it is located. Using zones and areas helps to organize the assessment and the design and application of countermeasures. These zones and areas include the buffer zone, perimeter, envelope, and interior:

- The **buffer zone** is the area immediately surrounding the facility that is outside of the facility's control. Depending on the neighborhood and uses of the adjacent land, certain factors can present threats and identify vulnerabilities for the facility.
- The **perimeter** is the boundary of the facility's property, which can be defined physically (e.g., by fencing) or virtually (e.g., by the property line). As the first point where the facility has control over the property, the perimeter is a key zone in providing proper security.

- The **envelope** includes a number of specific areas where people and materials either enter or exit. This is broadly defined and includes people, packages, information, vehicles, air, and utilities. As access points for the facility, the areas in the envelope often are where numerous specific vulnerabilities are present.
- The **interior** of the facility is the area past initial access control points where the tenant mission is carried out. Security considerations inside the facility must ensure that the occupants are provided a safe environment to carry out their duties and that critical facility systems are available to support operations.

A number of factors should be considered in planning a vulnerability assessment, including what method is available, the potential cost and effort needed to carry out the assessment, and the type of facility being assessed. The depth of analysis for this process will be determined by the type of assessment, or tier, selected at the beginning of the process, and should also include all applicable zones and areas for the facility. Vulnerability assessments should be conducted by experienced assessment specialists not responsible for the daily operation of the facility. This process allows for an unbiased and objective examination without preconceived notions, which increases the assessor's ability to identify specific vulnerabilities that may not ordinarily be identified by facility operators.

The activities necessary for conducting a vulnerability assessment include:

- Identification of a diverse and multi-disciplinary team of subject matter experts to conduct the assessment;
- Pre-meeting and preparation of a schedule and tentative agenda;
- Onsite meeting(s) with key staff upon arrival to review available information that may be useful for the assessment process;
- Walk-through of the key components of the asset, system, or network;
- Assessment background information request;
- Review of key documents; and
- Review of emergency procedures.

The following items should be examined during the vulnerability assessment:

- Key activities performed;
- Asset perimeter;
- Access control points;
- Security operations, including physical, cyber, and human systems;
- Primary point of entry of utilities and telecommunications;
- A cyber vulnerability assessment of the facility's access control, building automation, warning and security systems;
- Location and number of key staff;
- Systems necessary for the asset to function normally; and
- Whether an adversary can identify the asset and its importance.

It is important to ensure that countermeasures are functioning and operating as designed. Assessments should pay particular attention to potential cyber vulnerabilities, which can be exploited in many ways. Network "back doors" can exist in the form of modems, routers, wireless connections, and undocumented connections. Even without these obvious connections, connectivity exists if facilities permit the use of portable electronic devices and media, such as laptop computers, personal smart phones, tablets, and other devices. If employees, contractors, or visitors can carry any of these devices into the facility, and if onsite systems and networks permit the connection of these devices, then connectivity and the possibility of transferring data exists.

The assessment should produce a final report that details the findings and recommendations of the assessors and is tailored to the specific audience for which it is intended, whether that is the asset operator, senior department or agency management, auditors, or sector leadership. At a basic level, the final assessment report should include:

- Review of the methodology used to complete the assessment;
- Specific vulnerabilities likely to be exploited by natural or manmade hazards;
- Effectiveness of the existing countermeasures;
- Recommendations to strengthen or identify new countermeasures to increase resiliency; and
- Identification of additional resources that may be necessary to mitigate identified vulnerabilities.

Assessing Consequences

Consequence assessments provide information on the impact of damage or incapacitation to a facility. The focus of GFS consequence assessment efforts is to determine whether essential functions could be disrupted in the event of a natural or manmade disaster. This approach helps to determine impact not only to the GFS, but also across all sectors. In doing so, sector partners should give particular attention to their agency Mission Essential Functions (MEFs).

Consequence is defined by the sector as a successful undesired action or event to a facility. The initial screening process identified that a nationally significant consequence could be produced by disruption to the facility. This method filters out unrealistic attacks or disaster scenarios, concentrating focus on reasonable threats.

This full consequence assessment expands on the initial screening results by determining the severity of consequence likely to occur as a result of the incident for each of the consequence categories. These consequences likely to occur are then ranked using a worst reasonable case scenario. The consequence assessment is separated into four specific areas:

- **Human Safety:** Human consequences are the effect of an incident, event, or occurrence that results in injury, illness, or loss of life. This last category can be determined by measuring the number of fatalities resulting from an event. Estimating injuries and physical illness may require that thresholds and time periods be defined for those categories. For example, analysts may choose to only count injuries that occur immediately following the event that would result in death if left untreated or only consider people exposed to radiation or a chemical above a certain level.
- **Economic Impact:** This consequence category is the expected cost to the facility tenants to recover from an incident. In evaluating the likely economic impact of each threat, the SSA examines the direct financial loss that would reasonably occur based on each credible threat. This includes the assessed value of the facility as well as an estimate of the value of the items in the facility and the extent to which they would be damaged or destroyed as a result of the threat occurring. An economic consequence is the effect of an incident, event, or occurrence on the value of property or on production, trade, distribution, use of income, wealth, or commodities. Economic consequences are typically measured in monetary units and include direct asset damage, lost revenue, response cost, and lost business or market value. These consequences can include direct and indirect impacts and may be analyzed for their microeconomic business impacts or their broader macroeconomic impacts. When analyzing economic consequences, it should be stressed that such consequences cannot be assumed only to be negative. While the immediate economic impact in one area may be negative, the longer-term rebuilding effect may have some positive economic impact in a broader region. As with human consequences, analysts may need to set a threshold for what level of economic impact they will include in their assessment.
- **Mission:** A mission consequence is the effect of an incident, event, operation, or occurrence on the ability of an organization or group to meet a strategic objective or perform a function. To evaluate mission consequences, analysts should consider the impact of government agencies and civil service organizations on their ability to fulfill essential functions, such as law enforcement, transportation, banking, and social services. The event or incident may decrease the capabilities and capacity of these entities at the same time that the demand for their services increases. Consideration should also be given to how the change in mission functions affects larger national interests, such as security, economic prosperity, and the credibility of the Federal or state governments. Analysts will again have to consider the temporal and geographic scope of the risk assessment and set thresholds for mission consequences that will be assessed. Furthermore, since mission consequences are generally hard to estimate with any certainty, analysts should take care to properly caveat the results.

- **Psychological Impact:** Psychological consequences are the effects of an incident on the mental or emotional state of individuals or groups resulting in a change in perception or behavior. They can include both mental health impacts and psychosocial effects. When capturing psychological consequences, analysts may want to consider the fear, stress, depression, and other types of mental health disorders that could result from the incident, though this is often quite challenging. Changes in consumer behavior or perception, such as stockpiling of essential goods or shunning investing in an area, are another common psychological consequence that could be evaluated. Others include loss of confidence in government institutions and the market system; changes in compliance with government instructions; changes in social consciousness; greater information-seeking; and shifts in workplace, school, or event attendance. The social amplification of risk—meaning the distortion of a risk caused by public concern about the risk and/or about an activity contributing to the risk—can produce irrational behavior that exacerbates negative impacts.

Prioritization

Once the desired consequence categories have been identified, the next step is gathering data. The availability of data will depend on the types of events and incidents being assessed. For events that occur somewhat frequently, such as a Category II hurricane, existing databases, including insurance and other historical records, may be used as the basis for consequence estimates. Government databases, such as those created by the National Consortium for the Study of Terrorism and Responses to Terrorism, the Federal Emergency Management Agency, and the National Oceanic and Atmospheric Administration are rich information sources for terrorist attacks and natural disasters. Of course, analysts need to exercise caution in assuming that the consequences of future events will resemble the impacts of past ones.

A primary use of prioritization is to make informed resource allocation decisions, such as where protective programs should be instituted, the appropriate level of investment in these programs, and which protective measures offer the greatest return on investment. Because resources for critical infrastructure security and resilience are limited, risk analysis based on practical information must be completed before sound priorities can be established.

Departments and agencies should identify their critical assets/infrastructure; identify their primary and secondary mission essential functions; identify dependencies, interdependencies, and cascading effects; and then evaluate consequences with the loss of those functions through the Business Impact Analysis (BIA) process. The prioritization process applies to both physical and cyber assessment processes. Once critical infrastructure is identified a risk management methodology should be applied. This process should involve a multidisciplinary team of subject matter experts to identify, compile, analyze, and complete the assessment.

Implement Risk Management Activities

Protection of government facilities includes a combination of procedures, equipment, and personnel that span the preparedness spectrum. Protective programs must not only cover baseline levels of protection, they must also be scalable to enhance protection and resilience in response to facility-specific risk or changes in the National Threat Advisory System (NTAS). The GFS, by its very nature, focuses primarily on the deterrence and mitigation of threats; however, it also promotes a range of programs that are aimed to minimize consequences.

Overall security and resilience program planning and administration should ensure that protective programs are comprehensive, coordinated, and cost-effective. Planning is particularly important because different offices may be responsible for the protection of the various elements associated with a facility, as well as individual physical assets, cyber systems and networks, and government employees or other positions. Protection should be coordinated so that different offices' relationships to one another and their effects on the protection of the entire facility are taken into account.

Risk management activities are designed to assist the sector in reaching its goals by deterring threats, mitigating vulnerabilities, and minimizing consequences. These programs take a variety of forms depending on the specific focus of what is being protected. From visible and high-profile guard programs, to less noticed monitoring or password and

encryption protocols used to protect cyber systems and information, protective measures seek to reduce the specific risks faced by the GFS.

Protective programs cover not only baseline security measures, but also enhancements made in response to elevated threat, overall risk, or an incident, as well as actions taken during recovery and restoration. Therefore, protection of government facilities involves a comprehensive approach across the four components of the preparedness spectrum.

Protective programs and resilience strategies should be risk-based, implemented for a specific purpose, specifically tied to the facility or associated element, integrated with other protection and resilience measures, scalable, testable, and measurable. Some of the protective strategies applied within the GFS include:

- Physical access control systems, employee identification, visitor screening and escort systems that prevent unauthorized individuals from gaining access to sector facilities and networks.
- Surveillance systems, such as closed-circuit video and webcam capabilities, that monitor activity within and around a facility enable security personnel to identify and respond to disruptions and emergencies.
- Duress alarms or assistance stations, including call buttons in strategic locations throughout the facility, are used to alert security personnel in the event of an incident.
- Signage that instructs individuals how to report suspicious activity or hazardous situations and provides contact information.
- Facility lighting to illuminate and enhance visibility of perimeter and controlled areas.
- Crime Prevention through Environmental Design (CPTED) using natural and architectural features to protect a facilities setback as opposed to using ballads and barriers.
- Contract guards monitor and control entry posts, screen personnel and packages, patrol facility interior and perimeter. Should be armed when screening for weapons and meet minimum training requirements. Respond to emergencies, investigate and document suspicious/criminal activity.
- Agreements with local law enforcement to bolster security capabilities with high visibility patrols and emergency response times.
- DHS and the SSA also conduct periodic briefings and teleconferences, deliver information bulletins to address event-specific threats, develop coordinated responses, review lessons learned, and raise awareness of emerging threats. Past sessions have included teleconferences for situational awareness and post-event teleconferences covering lessons learned (i.e., the Boston Marathon Bombing; the Sandy Hook School Shooting; the Washington Navy Yard Shooting; Superstorm Sandy response and recovery; increased radicalization by terrorist organizations; and civil unrest in Ferguson, Missouri, and Baltimore, Maryland).

As the sector refines its understanding of mission interdependency, its role in promoting cybersecurity will evolve from the protection of physical assets to the integration of cyber systems resulting in the protection both against cybercrime and malicious cyber activity.

With the accelerating pace of technology, GFS partners should routinely assess their capabilities and refresh obsolete equipment and aging infrastructure through modernization programs and/or technical security upgrade projects. In-depth analyses of network intrusions should be performed to coordinate response to sophisticated cyberattacks. Additionally, penetration testing and network forensic analysis is used to deter and resolve major cyber threat issues. Through collaboration using the National Institute of Standards and Technology (NIST) Cybersecurity Framework, GFS partners should develop effective protective plans for their cyber assets/components. Partners are encouraged to share mitigating strategies, security practices, and lessons learned.

Logical Layers of Protection

The layered approach to protection also applies to cyber systems and networks. Technical or logical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices to protect against unauthorized access or misuse, help detect abuse and security violations, and provide security for applications.

Security technologies are implemented at each layer for two reasons: (1) to provide protective mechanisms appropriate to the entities being managed in each layer and (2) to ensure that there are many complementary protective measures to guard against attacks or flaws in any individual layer. Logical layers of protection and sample security mechanisms are shown in Figure 3 and Table 8.

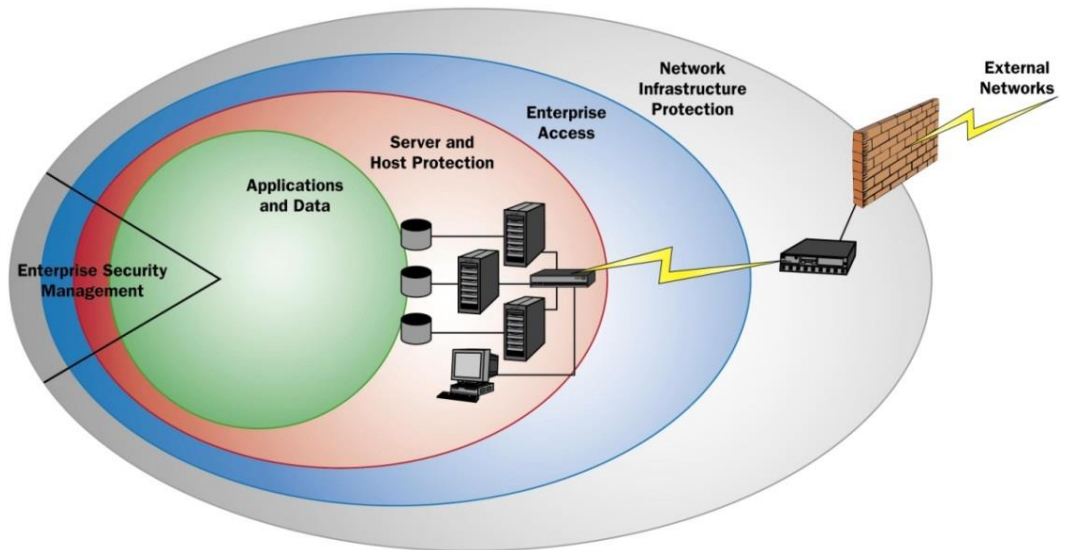


Figure 3: Cybersecurity Layers

Table 8: Logical Layer of Protection and Sample Security Mechanisms

Layer of Protection	Security Mechanism
Network infrastructure protection	<ul style="list-style-type: none"> Security provisions of routers, switches, and backbone network protocols. Virtual private networks. Security domains, firewalls, and demilitarized zones. Remote access protections.
Enterprise security management	<ul style="list-style-type: none"> Technologies for collection, analysis, and correlation of security-relevant data; assessing vulnerabilities; installing, patching, and managing configuration; detection, alerting, and responding to security events; and incident tracking, evidence gathering, and forensics investigation. Security-relevant aspects of services' continuity, including physical system location and protection, system and data backup, backup storage and protection, and recovery procedures and testing.
Enterprise access	<ul style="list-style-type: none"> Identification and authentication. Account management, password management, provisioning, and single sign on. Access controls based on user account, role, group, and other static or dynamic information. Policy definition, enforcement, and testing tools. Auditing. Non-repudiation services.
Server and host protection	<ul style="list-style-type: none"> Hardening of end systems and key infrastructure components. Integrity detection/assurance tools. Malicious code scanning and filtering. Host-based vulnerability assessment, prevention, detection, and monitoring. Host-based encryption and secure operating systems.
Application protection	<ul style="list-style-type: none"> Application-level identification, authentication, access control, encryption, and auditing. Application hardening, wrappers, and middleware security provisions. Application integrity detection/assurance and vulnerability assessment tools.
Data protection	<ul style="list-style-type: none"> Security services and mechanisms, such as database configuration and management. Database directory services. Database access control, auditing, event correlation, and alerting. Database survivability.

The Federal Information Protection Standard (FIPS) 199 provides the structure used by each Federal department and agency to categorize information and information systems in an inventory reported to Congress annually for compliance with the Federal Information Security Management Act (FISMA). The FIPS 199 “availability” measures impact of disruption only; it does not address contingency planning to ensure system accessibility. Use of FIPS 199 “availability” should be coordinated with individual department or agency continuity of operations planning personnel.

The IT or security department is responsible for the security and compliance of operational technology within the organization. NIST SP 800-82 Rev 2 provides guidance for securing operational technologies. In addition to designing and implementing a layered, defensive in-depth strategy, some networking and security best practices include:

- Developing security policies, procedures, training and educational material that applies specifically to the Industrial Control Systems (ICS).
- Considering ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, and deploying increasingly heightened security postures as the Threat Level increases.
- Addressing security throughout the lifecycle of the ICS, from architecture design to procurement, installation, maintenance, and decommissioning.
- Implementing a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Providing logical separation between the corporate and ICS networks (e.g., inspection firewall(s) between the networks).
- Employing a demilitarized zone (DMZ) network architecture (i.e., prevent direct traffic between the corporate and ICS networks).
- Ensuring that critical components are redundant and are on redundant networks.
- Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.
- Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
- Restricting physical access to the ICS network and devices.
- Restricting ICS user privileges to only those that are required to perform each person’s job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).
- Considering the use of separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts).
- Using modern technology, such as smart cards for Personal Identity Verification (PIV).
- Implementing security controls, such as intrusion detection software, antivirus software, and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.
- Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate.
- Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS.

Potential risks from a cyber incident within the GFS include:

- Allowing people to gain unauthorized access to facilities.
- Damaging temperature-sensitive equipment, such as in data centers.
- Causing life-safety systems, such as fire alarms or sprinklers, to give false alarms, fail to alarm in the event of an emergency, or other malfunctions that could result in injury or a loss of life.

- Disabling facilities due to lack of power or other environmental needs.
- Providing unauthorized access to information systems.
- Having to temporarily evacuate facilities.

DHS has established close relationships with state fusion centers by assigning Intelligence Officers (IO) to advocate for SLTT government agencies' intelligence requirements and to collaborate with Federal agencies to share intelligence products with SLTT government partners. In 2013, DHS offices addressing cyber and physical security collaborated to develop a joint risk assessment methodology, conducted at a GSA-owned facility, to determine vulnerabilities of automated building control systems. For 2015, the GFS continues to explore cyber/physical assessment tools and to develop a joint risk assessment methodology, which will be piloted at a GSA-owned facility, to determine vulnerabilities of automated building control systems. Lessons learned and best practices will be disseminated to the GCC when complete.

Overview of Sector R&D

Numerous ongoing R&D initiatives in both the public and private sectors have application to the GFS. Review of sector challenges, technology requirements, and current known R&D initiatives is conducted with sector partners representing the views of the sector. The product of this review includes a compilation of the current known initiatives relative to sector challenges and performance measures. This compilation is incorporated as part of the Sector CISR Protection Annual Report that impacts portions of the National Critical Infrastructure Protection (NCIP) R&D Plan.

The DHS Science and Technology Directorate (S&T) supports all 16 critical infrastructure sectors. S&T is the primary R&D liaison within DHS and provides Federal, State, local, tribal, and territorial officials with the technologies and capabilities to protect the homeland. This directorate also coordinates with SSAs to support development of sector R&D plans.

The National Infrastructure Security and Resilience Research and Development Plan (National CISR R&D Plan) required by PPD-21 was released in February 2015. The plan presents five overarching national critical infrastructure security and resilience R&D priority areas that are intended to inform R&D investments, promote innovation, and guide research across the critical infrastructure community:

- Develop the foundational understanding of critical infrastructure systems and systems dynamics;
- Develop integrated and scalable risk assessment and management approaches;
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure;
- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action; and
- Build a crosscutting culture of critical infrastructure security and resilience R&D collaboration.

Sectors will consider these five priority areas as inputs in its planning efforts to align its R&D activities and support implementation of the National CISR R&D Plan.

Sector R&D Requirements

GFS faces ongoing challenges to maintain awareness of adversaries' intent to launch strikes against government facilities and to remain vigilant in anticipation of and response to natural hazards. The sector has historically placed emphasis on protective actions as part of the prevention and protection elements of the preparedness spectrum. However, services performed by government are becoming increasingly interdependent across geographically dispersed facilities with increased reliance on the management of data, intelligence, and expert knowledge.

Along with the physical dangers to the sector, increased focus must be brought to protections against threats to mission security and service assurance by enhancing cybersecurity and resilience. This additional focus has a fundamental effect on the scope of the GFS' responsibility not only in maintaining the physical security of the facilities it includes, but also in embracing mission security, as well as rapid restoration and recovery. The Tritium Niagara cyber investigation exposed vulnerabilities to building automation system and identified massive global hacking rings; this indicates that all levels of infrastructure operations and management can and have been compromised. As a result, the GFS GCC should continue to increase information sharing and communications with sector partners and the IT community.

Considerations used to prioritize sector R&D requirements:

- Support for priority initiatives critical to sector operations
- Potential for dual use by other sectors or for the technology producer to achieve a better and more sustainable market position to ensure continued development and support of the required end product
- Affordability of the technology solution
- Operational practicality and effectiveness
- Environmental sustainability
- Legal, cultural, and aesthetic acceptance
- Capability to assess a vehicle at range and perform “diagnostic” and “defeat” procedures for any explosives—in particular, capability to non-intrusively detect vehicle-borne improvised explosive devices (IEDs)
- Capability to defeat vehicle-borne IEDs—in particular, non-explosive and standoff defeat
- Capability to screen people for explosives and weapons using technologies that allow higher detection rates with minimal disruptions to the flow of people—in particular, capability to detect person-borne IEDs from a standoff distance
- Capability to defeat person-borne and “leave-behind” IEDs
- Capability to provide emergency managers with seamless data, voice, and video information for enhanced situational awareness in major and minor crises
- Improved screening and examination by nonintrusive inspection—in particular, the ability to detect homemade explosives, liquid and inorganic explosives, toxic industrial chemicals, and chemical warfare agents
- Optimization of canine explosive detection capability
- Improved cross-agency reporting of suspicious activity—in particular, technologies that would improve real-time awareness
- Data fusion from law enforcement, the intelligence community, and other sources to support a user-defined operating picture—in particular, technologies to support monitoring by FPS MegaCenters of alarm systems, closed-circuit television, and wireless dispatch communications
- Enhanced capability to identify individuals and verify the professional credentials of individuals in both preplanned and developing event
- Management of user identities, rights, and authorities—in particular, technologies and standards to enable external identity adjudication
- Information sharing within and across sectors on terrorist threats, including the improvement of situational awareness and decision support
- Predictive analytics capability to correlate data and information for recognizing and predicting criminal and terrorist activity—in particular, the capability to predict participants and locations for IED attacks

- Capability to acquire biometrics information in challenging operating environments and to provide real-time positive verification of an individual’s identity using multiple biometrics
- Mobile biometrics screening capabilities, including handheld 10-fingerprint, face, and iris capture
- High resolution analytical tools to accurately model and quantify interdependencies and cascading consequences as disruptions occur within the sector and across dependent sectors
- Effective and affordable blast analysis protection for critical infrastructure, and improved understanding of blast failure mechanisms and protection measures
- Effective and affordable electromagnetic pulse hardening solutions
- Advanced, automated, and affordable monitoring and surveillance—in particular decision support systems and mitigation strategies to prevent disruptions and build in resilience
- Entry and access portals—Personal identity verification
- Insider threats—Insider threat and automated scene awareness
- Analysis and decision support systems—Modeling of infrastructure interdependencies and cascading effects
- Response, recovery, and reconstitution—Bottom-up modeling of evacuation methodologies
- Weakness and vulnerabilities of building devices/automated systems

4.2 Critical Infrastructure and National Preparedness

Presidential Policy Directive 8 (PPD-8) is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyberattacks, pandemics, and catastrophic natural disasters. Our national preparedness is the shared responsibility of all Federal, State, local, tribal, and territorial governments, the private and nonprofit sectors, and individual citizens. Everyone can contribute to safeguarding the Nation from harm. As such, while this directive is intended to galvanize action by the Federal Government, it is also aimed at facilitating an integrated, all-of-Nation, capabilities-based approach to preparedness.

The National Preparedness System outlines an organized process for the whole community to achieve the National Preparedness Goal. The National Preparedness System integrates efforts across the five preparedness mission areas—Prevention, Protection, Mitigation, Response, and Recovery—in order to achieve the goal of a secure and resilient Nation. The National Protection Framework, part of the National Preparedness System, sets the strategy and doctrine for how the whole community builds, sustains, and delivers the protection core capabilities identified in the National Preparedness Goal in an integrated manner with the other mission areas. The second edition of the National Protection Framework reflects the insights and lessons learned from real-world incidents and the implementation of the National Preparedness System. There are many departments, agencies, and jurisdictions within the GFS community that offer programs that support the five preparedness mission areas of critical infrastructure security and resilience:

- **Prevention:** The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. As defined by PPD-8, the term “prevention” refers to preventing imminent threats.
- **Protection:** The capabilities necessary to secure the homeland against acts of terrorism and human-caused or natural disasters.
- **Mitigation:** The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.
- **Response:** The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.
- **Recovery:** The capabilities necessary to assist communities affected by an incident to recover effectively.

5 MEASURING EFFECTIVENESS

The GFS continues to focus on implementing long-term government facility risk management strategies to increase facility protection and resilience; manage and develop capabilities in order to maximize efficient use of resources; promote timely and accurate information sharing; and analyze infrastructure dependencies, interdependencies, and cascading effects. During incidents, GFS identify and assesses consequences to events affecting infrastructure. Following incidents and exercises, GFS learns, adapts, and shares best practices across the sector. Strengthening sector development and the delivery of technical assistance, training and education, and identifying R&D needs.

Progress toward achieving sector goals is assessed by measuring the performance of protective programs, assessments, and progress reporting. Such measures inform the risk management efforts of partners throughout the critical infrastructure community and help build a national picture of progress toward the vision of the NIPP. SSAs encourage partners to participate in data calls, working groups, GCC meetings, and other sector-specific reporting mechanisms. The SSA will continue to share information with all stakeholders; identifying sector vulnerabilities, strategies, and best practices.

Regular review of progress allows sector partners to quantify the benefits achieved by specific activities, incorporate improvements into protective programs where needed, and inform future resource allocation decisions that focus on highest priority facilities.

Reporting

PPD-21 requires each SSA to provide the Secretary of Homeland Security with annual reports that serve as a primary tool for assessing performance and reporting progress. The National Annual Report (NAR) provides a platform for each sector to communicate protection performance, progress, and priorities to sector partners. This information is compiled by DHS and submitted to the President of the United States.

















Consistent with this requirement, DHS provides the SSAs with reporting guidance and templates that include requests for specific information, such as sector protection priorities, requirements, and resources. The following elements are included to help inform the prioritization of resource allocation recommendations:

- Priorities and annual goals for sector security and resilience, as well as associated gaps;
- Current sector-specific requirements for security and resilience activities and programs based on risk, need, and any other drivers, such as regulations and Presidential directives;
- Projected requirements for the sector, with an emphasis on anticipated gaps or shortfalls in funding for the sector or national critical infrastructure security and resilience; and
- The disruption of sector assets that would cause regionally or nationally significant impacts under both steady-state and incident conditions.

Sector input into this process is coordinated by the SSA. Sector partners identify and report on their most critical facilities/infrastructure, identifying successes and challenges, in protecting these facilities and assets. Top tier critical assets are identified by assessing whether they meet the baseline level of protection and whether vulnerabilities can be mitigated.

By identifying their most critical facilities and challenges, resources can be applied where they best contribute to mitigate risk, reduce vulnerabilities, deter threats, and minimize consequences. The NAR process will be broadened to the next level of critical assets as the top tier is completed.

Table 4: Sector Priorities mapped to the Joint National Priorities and aligned with the NIPP Goals

Government Facilities Sector Priorities	Joint National Priorities					NIPP Goals
	Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision Making	Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities	
A Progressively Implement a GFS Risk Management Program						Assess and analyze risks to critical infrastructure (T, V, C) to inform risk management activities.
B Organize and Partner for GFS Security and Resilience						Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery.
C Integrate GFS Security and Resilience as Part of the Homeland Security Mission						Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
D Manage and Develop the Capabilities of the GFS						Promote learning and adaptation during and after incidents and exercises.
E Maximize Efficient use of Recourses for GFS Security and Resilience						Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.

APPENDIX A

Glossary of Terms

Term	Definition
All Hazards	The term “all hazards” means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure. (Source: PPD-21, 2013)
Asset	Person, structure, facility, information, material, or process that has value. (Source: DHS Lexicon, 2010)
Best Practice	A best practice evaluates what already exists, what lessons have been learned, and what would be changed or avoided to make it possible to achieve defined goals. Sometimes best practices may be adopted from other successful agencies.
Business Continuity	Activities performed by an organization to ensure that during and after a disaster the organization’s essential functions are maintained uninterrupted, or are resumed with minimal disruption. (Source: Adapted from the 2009 NIPP)
Cascading Effects	Sequence of events/incidents in which each event produces or causes the onset of the next.
Consequence	The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with economic impacts, both direct and indirect, and other negative outcomes to society. (Source: Adapted from DHS Lexicon, 2010)
Continuous Process Improvement	Structured approach for analyzing how an organization is currently doing work and how it can improve processes to do the job more efficiently and effectively on an ongoing basis.
Control Systems	Computer-based systems used within many infrastructure sectors and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include SCADA systems, Process Control Systems, and Distributed Control Systems. (Source: 2009 NIPP)
Core Capabilities	Identified by the National Preparedness Goal and grouped in five preparedness mission areas, the core capabilities consist of 31 distinct critical elements needed to achieve the goal. (Source: FEMA.gov/Core-Competencies)
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source: §1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e)))
Critical Infrastructure Community	Critical infrastructure owners and operators, both public and private; Federal departments and agencies; regional entities; SLTT governments; and other organizations from the private and nonprofit sectors with a role in securing and strengthening the resilience of the Nation’s critical infrastructure and/or promoting practices and ideas for doing so. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
Critical Infrastructure Cross-Sector Council	Private sector council that comprises the chairs and vice chairs of the SCCs. This council coordinates cross-sector issues, initiatives, and interdependencies to support critical infrastructure security and resilience. (Source: Adapted from the 2009 NIPP)

Term	Definition
Critical Infrastructure Information (CII)	Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems.
Critical Infrastructure Owners and Operators	Those entities responsible for day-to-day operation and investment of a particular critical infrastructure entity. (Source: Adapted from the 2009 NIPP)
Critical Infrastructure Partner	Those Federal and SLTT governmental entities, public and private sector owners and operators and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share responsibility for securing and strengthening the resilience of the Nation's critical infrastructure. (Source: Adapted from the 2009 NIPP)
Critical Infrastructure Partnership Advisory Council (CIPAC)	Council established by DHS under 6 U.S.C. §451 to facilitate effective interaction and coordination of critical infrastructure activities among the Federal Government, the private sector, and SLTT governments. (Source: CIPAC Charter)
Critical Infrastructure Risk Management Framework	A planning and decision-making framework that outlines the process for setting goals and objectives, identifying infrastructure, assessing risks, implementing risk management activities, and measuring effectiveness to inform continuous improvement in critical infrastructure security and resilience. (Source: Adapted from the 2009 NIPP)
Critical Infrastructure Sectors	A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; NIPP 2013 addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
Cybersecurity	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: 2009 NIPP)
Cyber System	Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services; examples include business systems, control systems, and access control systems. (Source: 2009 NIPP)
Dependency	The one-directional reliance of an asset, system, network, or collection thereof—within or across sectors—on an input, interaction, or other requirement from other sources in order to function properly. (Source: 2009 NIPP)
Executive Order 13636	Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013)
Emergency Support Functions (ESF)	The primary, but not exclusive, Federal coordinating structures for building, sustaining, and delivering the response core capabilities. ESFs are vital for responding to Stafford Act incidents but also may be used for other incidents. (Source: National Response Framework, 2013)
Enterprise Risk Management	A comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision-making for managing risk that may hinder an organization from achieving its objectives.
Event	Planned, non-emergency activity occurring in a particular place during a particular interval of time.
Federal Departments and Agencies	Any authority of the United States that is an “agency” under 44 U.S.C. §3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. §3502(5). (Source: PPD-21, 2013)

Term	Definition
Federal Interagency Operational Plans (FOIPs)	One for each preparedness mission area, FOIPs describe how the Federal government aligns resources and delivers core capabilities. (Source: FEMA.gov/federal-interagency-operational-plans)
Federal Senior Leadership Council (FSLC)	The objective of the FSLC is to drive enhanced communications and coordination among Federal departments and agencies that have a role in implementing PPD-21 and the NIPP. The members of the FSLC include the Sector-Specific Agencies for each of the critical infrastructure sectors as well as several additional agencies that have infrastructure security responsibilities.
Function	Service, process, capability, or operation performed by an asset, system, network, or organization. (Source: DHS Lexicon, 2010)
Fusion Center	A State and major urban area focal point for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government, SLTT, and private sector partners. (Source: Adapted from the DHS Lexicon, 2010)
Government Coordinating Council (GCC)	The government counterpart to the Sector Coordinating Council for each sector established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government (Federal and SLTT) as appropriate to the risk and operational landscape of each sector. (Source: 2009 NIPP)
Hazard	Natural or manmade source or cause of harm or difficulty. (Source: DHS Lexicon, 2010)
Homeland Security Information Network (HSIN)	A national, secure, and trusted web-based portal for information sharing and collaboration between Federal, State, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.
Homeland Security Information Network-Critical Infrastructure (HSIN-CI)	One series of Community of Interest (COI) portals available on HSIN; The HSIN-CI COIs are used by the Department of Homeland Security and other Federal, State, local, tribal, territorial, and private sector partners to securely share data, techniques, and best practices, and to support systematic, risk-based planning in an effort to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's critical infrastructure. (Source: DHS.gov/HSIN)
Impact	Measure of effect or influence of an action, person, or thing on another
Incident	An occurrence, caused by either human action or natural phenomenon, that may cause harm and require action, which can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, cyberattacks, cyber failure/accident, and other occurrences requiring an emergency response. (Source: DHS Lexicon, 2010)
Incident Management	Management and coordination of prevention, protection, and emergency management activities associated with a specific threat or an actual occurrence.
Indirect Consequence	Effect that is not a direct consequence of an event, incident, or occurrence, but is caused by a direct consequence, subsequent cascading effects, and/or related decisions.
Information Sharing and Analysis Centers (ISACs)	Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (Source: Presidential Decision Directive 63, 1998)

Term	Definition
Information Sharing and Analysis Organization (ISAO)	Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of: <ul style="list-style-type: none"> • Gathering and analyzing cybersecurity information; • Distributing cybersecurity information; and • Collaborating with members; customers; other ISAOs; or other private sector, Federal, State, local, tribal, territorial, and international entities to respond to cyber threats and mitigate cyber risk.
Information Technology System	An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems. [NIST 800-53 rev 4]
Infrastructure	The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (Source: DHS Lexicon, 2010)
Interdependency	Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions. (Source: DHS Lexicon, 2010)
The Joint Information Management Center (JIMC)	A joint information sharing and operation center managed by FPS and GSA.
Joint National Priorities	The joint national priorities provide a common focal point for partnership efforts, developed through cross-sector information sharing and collaborative working group sessions, the joint national priorities build upon an evaluation of emerging risks, known capability gaps, resource availability, and best practices.
Joint Terrorism Task Forces (JTTFs)	Local task forces of highly trained Federal, State, and local law enforcement and intelligence agencies led by the FBI and established to collect terrorism-related intelligence and conduct investigations. The local FBI JTTFs receive and resolve reports of possible terrorism activity submitted by private industry partners and the public. (Source: Federal Bureau of Investigation, 2013)
Lesson Learned	Knowledge derived from a response to an event that will affect mitigation activities.
Lessons Learned Information Sharing (LLIS.gov)	A U.S. Department of Homeland Security/Federal Emergency Management Agency information and collaboration resource that helps first responders, emergency managers, and homeland security officials prepare for, protect against, respond to, recover from, and mitigate terrorist attacks, natural disasters, and other emergencies. LLIS.gov provides Federal, State, Local, Tribal, and Territorial responders and managers from all disciplines with a wealth of information and front-line expertise on effective planning, training, and operational practices. (Source: LLIS.gov)
Likelihood	Chance of something happening, whether defined, measured, or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities.
Mitigation	One of the five Preparedness Mission Areas defined by PPD-8; capabilities necessary to reduce loss of life and property by lessening the impact of disasters. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)

Term	Definition
National Annual Report	The plan specifies the key initiatives, milestones, and metrics required to achieve the Nation's critical infrastructure security and resilience mission, sets forth a comprehensive risk management framework, and clearly defines roles and responsibilities for the Department of Homeland Security (DHS), Federal Sector-Specific Agencies (SSAs), and other Federal, State, local, tribal, territorial, and private sector security partners.
National Cybersecurity and Communications Integration Center (NCCIC)	The national cyber critical infrastructure center, as designated by the Secretary of Homeland Security, which secures Federal civilian agencies in cyberspace; provides support and expertise to private sector partners and SLTT entities; coordinates with international partners; and coordinates the Federal Government mitigation and recovery efforts for significant cyber and communications incidents. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
National Cyber Investigative Joint Task Force	The multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations with representation from Federal agencies, including DHS, and State, local, and international law enforcement partners. (Source: FBI Web site, www.fbi.gov)
National Infrastructure Coordinating Center (NICC)	The national physical critical infrastructure center, as designated by the Secretary of Homeland Security, which coordinates a national network dedicated to the security and resilience of critical infrastructure of the United States by providing 24/7 situational awareness through information sharing and fostering a unity of effort. (Source: DHS.gov/national-infrastructure-coordinating-center)
National Infrastructure Protection Plan (NIPP)	National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes. (Source: DHS.gov/national-infrastructure-protection-plan)
National Operations Center (NOC)	A DHS 24/7 operations center responsible for providing real-time situational awareness and monitoring of the homeland, coordinating incident response activities, and, in conjunction with the Office of Intelligence and Analysis, issuing advisories and bulletins concerning threats to homeland security, as well as specific protective measures. (Source: DHS.gov/office-operations-coordination)
National Preparedness	The actions taken to plan, organize, equip, train, exercise, build, and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. (Source: PPD-8, 2011)
National Preparedness Goal	The cornerstone of implementation of Presidential Policy Directive 8: National Preparedness (PPD-8), which describes the Nation's approach to preparing for the threats and hazards that pose the greatest risk to the security of the United States. Success is defined as "A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." (Source: National Preparedness Goal, 2011)
National Protection and Programs Directorate (NPPD) – (DHS/NPPD)	NPPD leads the DHS mission to reduce risk to the Nation's critical physical and cyber infrastructure through partnerships that foster collaboration and interoperability. (Source: DHS FY13 Budget Guidance)
National Preparedness Report (NPR)	Required annually by Presidential Policy Directive 8: National Preparedness. The National Preparedness Report summarizes national progress in building, sustaining, and delivering the 31 core capabilities outlined in the National Preparedness Goal.
National Preparedness System	Outlines an organized process for everyone in the whole community to move forward with their preparedness activities and achieve the National Preparedness Goal. (Source: http://www.fema.gov/national-preparedness-system)

Term	Definition
National SAR (Suspicious Activity Reporting) Initiative (NSI)	A joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and State, Local, Tribal, and Territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. (Source: NSI.ncirc.gov)
Natural Hazard	Source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena.
Network	A group of components that share information or interact with each other to perform a function. (Source: 2009 NIPP)
Nongovernmental Organization (NGO)	An entity with an association that is based on interests of its members, individuals, or institutions that has no statutory ties with a government.
Office of Cyber Security and Communications (CS&C) – (NPPD/CS&C)	The mission of CS&C is to enhance the security, resilience, and reliability of the Nation's cyber and communications infrastructure.
Office of Cyber and Infrastructure Analysis (OCIA) – (NPPD/OCIA)	OCIA's mission is to support efforts to protect the Nation's critical infrastructure through an integrated analytical approach evaluating the potential consequences of disruption from physical or cyber threats and incidents.
Office of Infrastructure Protection (IP) – (NPPD/IP)	The mission of IP is to lead the national effort to protect critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.
Partnership	Close cooperation between parties having common interests in achieving a shared vision. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
Preparedness	Activities necessary to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents.
Preparedness Mission Areas	Identified by the National Preparedness Goal, the five preparedness mission areas are Prevention, Protection, Mitigation, Response, and Recovery. These five mission areas serve as an aid in organizing our national preparedness activities, and do not constrain or limit integration across mission areas and core capabilities, which by their nature are highly interdependent and applicable to any threat or hazard. (Source: National Preparedness Goal, 2011)
Presidential Policy Directive	Directives used to promulgate Presidential decisions on national security matters. (Source: WhiteHouse.gov)
Presidential Policy Directive 8 (PPD-8)	Facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (Source: PPD-8, 2011)
Presidential Policy Directive 21 (PPD-21)	Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and SLTT entities to enhance the security and resilience of critical infrastructure. (Source: PPD-21, 2013)
Prevention	Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. (Source: PPD-8, 2011)
Private Sector	Individuals and entities, including for-profit and non-profit, which are not part of any government.

Term	Definition
Protected Critical Infrastructure Information (PCII)	All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive; all information submitted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise. (Source: CII Act of 2002, 6 U.S.C. § 131)
Protection	Those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. (Source: PPD-8, 2011)
Protective Measures	Steps taken before, during, or after an incident designed to prevent, minimize, or contain impact of incident.
Protective Security Advisors (PSAs)	Trained critical infrastructure protection and vulnerability mitigation subject matter experts. Regional Directors are supervisory PSAs responsible for the activities of eight or more PSAs and geospatial analysts who ensure all Office of Infrastructure Protection critical infrastructure security and resilience programs and services are delivered to State, local, tribal, and territorial stakeholders and private sector owners and operators. (Source: DHS.gov/protective-security-advisors)
Protective Security Coordination Division (PSCD)	PSCD's mission is to provide strategic coordination and field operations support to reduce risk to the Nation's critical infrastructure from a terrorist attack or natural disaster. PSCD programs help critical infrastructure owners and operators and state and local responders assess vulnerabilities, interdependencies, capabilities, and incident consequences; develop, implement, and provide national coordination for protective programs; and facilitate critical infrastructure response to and recovery from all hazards. (Source: DHS.gov/about-protective-security-coordination-division)
Public-Private Partnership	A contractual arrangement between a public agency (Federal, State, or local) and a private sector entity. Through this agreement, the skills and assets of each sector (public and private) are shared in delivering a service or facility for the use of the general public. (Source: National Council for Public-Private Partnerships)
Readiness	A condition of being prepared and capable to act or respond as required
Recovery	Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources. (Source: PPD-8, 2011)
Recovery Support Functions (RSF)	Coordinating structures for key functional areas of assistance during recovery operations. RSFs support local governments by facilitating problem solving, improving access to resources, and fostering coordination among State and Federal agencies, nongovernmental partners, and stakeholders. (Source: National Disaster Recovery Framework, 2011)
Redundancy	Additional or alternative systems, subsystems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, subsystem, asset, or process.
Regional	Entities and interests spanning geographic areas ranging from large multi-State areas to metropolitan areas and varying by organizational structure and key initiatives, yet fostering engagement and collaboration between critical infrastructure owners and operators, government, and other key stakeholders within the given location. (Source: Regional Partnerships: Enabling Regional Critical Infrastructure Resilience, RC3, March 2011)
Regional Consortium Coordinating Council	Comprises regional groups and coalitions around the country engaged in various initiatives to advance critical infrastructure security and resilience in the public and private sectors. (Source: Adapted from the 2009 NIPP)

Term	Definition
Regional Resiliency Assessment Program (RRAP)	An assessment of specific critical infrastructure and a regional analysis of the surrounding infrastructure. The RRAP evaluates critical infrastructure on a regional level to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective, identifying dependencies, interdependencies, cascading effects, resilience characteristics, and gaps. (Source: DHS.gov/regional-resiliency-assessment-program)
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Source: PPD-21, 2013)
Response	Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. (Source: PPD-8, 2011)
Risk	The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (Source: DHS Lexicon, 2010)
Risk Acceptance	An explicit or implicit decision not to take an action that would affect all or part of a particular risk.
Risk Analysis	A systematic examination of the components and characteristics of risk; in practice, risk analysis is generally conducted to produce a risk assessment.
Risk Assessment	A product or process evaluating information based on a set of criteria that assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision-making.
Risk Assessment Tool	An activity, item, or program that contributes to determining and evaluating risks.
Risk Avoidance	Strategies or measures taken that effectively remove exposure to a risk.
Risk Communication	An exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to act appropriately in response to an identified risk.
Risk-Informed Decision-Making	The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors. (Source: 2009 NIPP)
Risk Management	A process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.
Risk Mitigation	An application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences.
Risk Tolerance	A degree to which an entity is willing to accept risk.
Risk Transfer	An action taken to manage risk that shifts some or all of the risk to another entity, asset, system, network, or geographic area.
Risk-Based Decision Making	A determination of a course of action predicated primarily on the assessment of risk and the expected impact of that course of action on that risk.
Risk-Informed Decision Making	A determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, as well as other relevant factors. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
Sector	A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; the National Plan addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: Adapted from the 2009 NIPP)

Term	Definition
Sector Coordinating Council (SCC)	The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. They serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (Source: Adapted from the 2009 NIPP)
Sector Outreach and Programs Division (SOPD)	SOPD's mission is to build, align, and leverage national public-private stakeholder partnerships and partnership programs to enhance critical infrastructure security and resilience.
Sector-Specific Agency (SSA)	A Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise, as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (Source: PPD-21, 2013)
Sector-Specific Plans (SSP)	Planning documents that complement and tailor application of the National Infrastructure Protection Plan to the specific characteristics and risk landscape of each critical infrastructure sector. SSPs are developed by the SSAs in close collaboration with the SCCs and other sector partners. (Source: Adapted from the 2009 NIPP)
Secure/Security	Reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. (Source: PPD-21, 2013)
Stakeholder	A person, group, or organization that has interest or concern in an organization. Stakeholders can affect or be affected by the organization's actions, objectives and policies. (Source: Businessdictionary.com)
State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)	The SLTTGCC serves as a forum to ensure that State, local, tribal, and territorial homeland security partners are fully integrated as active participants in national critical infrastructure security efforts, and to provide an organizational structure to coordinate across jurisdictions on critical infrastructure security and resilience guidance, strategies, and programs. The SLTTGCC will provide the State, local, tribal, or territorial perspective or feedback on a wide variety of critical infrastructure issues.
Steady State	The posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents. (Source: DHS Lexicon, 2010)
Strategic Driver	Forces that shape an organization's high level plan to achieve one or more goals under conditions of uncertainty.
Strategic Goal	A statement of aim or purpose in a strategic plan that articulates what is needed to achieve an objective.
Strategic National Risk Assessment (SNRA)	An assessment executed by the DHS Office of Risk Management and Analysis in support of Presidential Policy Directive 8 (PPD-8), which calls for the creation of a National Preparedness Goal, a National Preparedness System, and a National Preparedness Report. (Source: DHS.gov/strategic-national-risk-assessment-snra)
Strategy	A statement of a course of action(s) to be taken in order to execute task(s), achieve objective(s) or goal(s), fulfill mission(s), or realize end state(s) based on existing or expected resources.
Suspicious Activity Reporting (SAR)	An official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.
System	Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (Source: DHS Lexicon, 2010)
Terrorism	Premeditated threat or act of violence against noncombatant persons, property, and environmental or economic targets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives. (Source: DHS Lexicon, 2010)

Term	Definition
Threat	One of three functional elements of risk, threat is an indication of potential harm to life, information, operations, the environment, and/or property. It may be a natural or human created occurrence and includes capabilities, intentions, and attack methods of adversaries used to exploit circumstances or occurrences with the intent to cause harm.
Threat and Hazard Identification and Risk Assessment (THIRA)	A tool that allows a regional, State, or urban area jurisdiction to understand its threats and hazards and how the impacts may vary according to time of occurrence, season, location, and other community factors. This knowledge helps a jurisdiction establish informed and defensible capability targets for preparedness. (Source: FEMA.gov/threat-and-hazard-identification-and-risk-assessment)
Threat Assessment	A product or process of evaluating information based on a set of criteria for entities, actions, or occurrences, whether natural or manmade, that has or indicates the potential to harm life, information, operations, and/or property.
Unacceptable Risk	A level of risk at which, given costs and benefits associated with further reduction measures, action is deemed to be warranted at a given point in time.
Value Proposition	A statement that outlines the business and national interest in critical infrastructure security and resilience actions and articulates the benefits gained by partners through collaborating in the mechanisms described in the National Plan. (Source: Adapted from the 2009 NIPP)
Vulnerability	A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (Source: DHS Lexicon, 2010)
Vulnerability Assessment	A product or process of identifying susceptibility or exposure to hazards of an area of concern; includes entities, assets, systems, networks, or geographic areas.

APPENDIX B

List of Acronyms and Abbreviations

BZPP	Buffer Zone Protection Program	GFS	Government Facilities Sector
C³	Critical Infrastructure Cyber Community	GSA	General Services Administration
CBR	Chemical, Biological, and Radiological	HHS	Health Human Services
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive	HSAs	Homeland Security Advisors
C-Cubed	Critical Infrastructure Cyber Community	HSIN	Homeland Security Information Network
CET	Continuity Evaluation Tool	HSIN-CI	Homeland Security Information Network-Critical Infrastructure
CFDI	Critical Foreign Dependencies Initiative	HSPD	Homeland Security Presidential Directive
CIO	Chief information Officer	HUD	Housing and Urban Development
CIPAC	Critical Infrastructure Partnership Advisory Council	ICAM	Identity, Credential and Access Management
COG	Continuity of Government	ICS	Industrial Control Systems
COGCON	Continuity of Government Condition	ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
COI	Community of Interest	IP	Office of Infrastructure Protection
COOP	Continuity of Operations Plan	IRVS	the Integrated Rapid Visual Screening
CS&C	Office of Cybersecurity and Communications	ISAC	Information Sharing and Analysis Organization
CSCSWG	Cross Sector Cyber Security Workgroup	ISAO	Information Sharing and Analysis Organization
CSET	Cyber Security Evaluation Tool	ISC	Interagency Security Committee
CSO	Chief Security Officer	IT	Information Technology
DBT	Design Basic Threat	JFO	Joint Field Office
DHS	Department of Homeland Security	JIMC	Joint Information Management Center
DOD	Department of Defense	LEO	Law Enforcement Online
DOE	Department of Energy	MEF	Mission Essential Functions
DOI	Department of Interior	MIST	Modified Infrastructure Survey Tool
DOJ	Department of Justice	NC4	National Center for Crisis and Continuity Coordination
DOS	Department of State	NCCIC	National Cybersecurity and Communications Integration Center
DOT	Department of Transportation	NCIPP	National Critical Infrastructure Prioritization Program
ECS	Enhanced Cyber Security	NCPC	National Crime Prevention Council
EF	Education Facilities	NCS	National Communications System
EO	Executive Order	NEF	National Essential Function
EOC	Emergency Operations Center	NICC	National Infrastructure Coordination Center
EPA	Environment Protection Agency	NIPP	National Infrastructure Protection Plan
FAS	Federal Acquisition Service	NIST	National Institute of Standards and Technology
FBI	Federal Bureau of Investigation	NMI	National Monuments and Icons Subsector
FCD	Federal Continuity Directive	NOC	National Operations Center
FedRAMP	Federal Risk and Authorization Management Program	NPPD	National Protection and Programs Directorate
FEMA	Federal Emergency Management Agency	NRCC	National Response Coordination Center
FSA	Facility Security Assessment	NRF	National Response Framework
FCD	Federal Continuity Directive	NSI	Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)
FSL	Facility Security Level	OMA	Office of Mission Assurance
GCC	Government Coordinating Council	OP	Operation Center

PBS	Public Buildings Service	SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
PMEF	Primary Mission Essential Function	SNRA	Strategic National Risk Assessment
PMI	Protection Measures Index	SSA	Sector-Specific Agency
PPD	Presidential Policy Directive	SSP	Sector-Specific Plan
PSA	Protective Security Advisor	S&T	Science and Technology Directorate
R&D	Research and Development	THIRA	Threat and Hazard Identification and Risk Assessment
RRAP	Regional Resiliency Assessment Program	US-CERT	United States Computer Emergency Response Team
RRCC	Regional Response Coordination Center	USACE	United States Army Corps Of Engineers
SAR	Suspicious Activity Reporting	USCG	United States Coast Guard
SBA	Small Business Administration	USDA	United States Department of Agriculture
SCC	Sector Coordinating Council		

APPENDIX C

Summary of Relevant Authorities

Authorities include statutes, regulations, executive orders, Presidential directives and decision documents, circulars, memoranda, building codes, zoning standards, and other regulatory or authoritative measures. This list of authorities provides examples specific to GFS. Because the NIPP includes a complete list of authorities relevant to infrastructure protection, they are not repeated here.

Federal Statutes and Regulations	
Critical Infrastructure Information Act 2002	H.R. 1772: Criminal Code Modernization and Simplification Act of 2009
Cyber Security Research and Development Act of 2002	H.R. 1292 – To amend title I of the Omnibus Crime Control and Safe Streets Act of 1968 to establish a National White Collar Crime Center grants program
Disaster Mitigation Act of 2000	Information Technology Management Reform Act of 1996
Facility Standards for Records Storage Facilities, 36 Code of Federal Regulations (CFR) 1228	Intelligence Reform and Terrorism Prevention Act of 2004
Federal Information Security Management Act of 2002	National Archives and Records Administration of 1984
Federal Management Regulation, 41 CFR 102	National Security Act of 1947
Federal Property and Administrative Services Act of 1949	Occupational Safety and Health Act of 1970
Fire Administration Authorization Act of 1992	Omnibus Diplomatic Security and Antiterrorism Act of 1986
Freedom of Information Act	Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (Act of 2003)
Government Management Reform Act of 1994	Public Buildings Act of 1959
Government Performance and Results Act of 1993	Public Health Security and Bioterrorism Preparedness and Response Act
Homeland Security Act of 2002	S. 1438: Fostering a Global Response to Cyber Attacks Act
Presidential Directives	
Presidential Policy Directive 1: Organization of the National Security Council System	
Presidential Policy Directive 8: National Preparedness	
Presidential Policy Directive 21: Critical Infrastructure Security and Resilience	
HSPD-1: Organization and Operation of the Homeland Security Council	
HSPD-3: Homeland Security Advisory System	
HSPD-5: Management of Domestic Incidents	
HSPD-6: Integration and Use of Screening Information	
HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection Replaced by PPD 21	
HSPD-8: National Preparedness	
HSPD-11: Comprehensive Terrorist-Related Screening Procedures	
HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors	
HSPD-19: Combating Terrorist Use of Explosives in the United States	
HSPD-20/National Security Presidential Directive 51(NSPD-51): National Continuity Policy	
HSPD-23: National Cyber Security Initiative	

Executive Orders

Executive Order 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions

Executive Order 12906: Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure

Executive Order 12977: Interagency Security Committee

Executive Order 13327: Federal Real Property Asset Management

Executive Order 13231: Critical Infrastructure Protection in the Information Age

Executive Orders 13402 and 13414: Strengthening Federal Efforts To Protect Against Identity Theft

Executive Order 13407: Public Alert and Warning System

Executive Order 13411: Improving Assistance for Disaster Victims

Executive Order 13434: National Security Professional Development

Executive Order 13636: Improving Critical Infrastructure Cyber-Security

National Strategies

National Intelligence Strategy

National Strategy for Combating Terrorism (February 2003)

National Strategy for Homeland Security (July 2002)

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003)

National Strategy to Combat Weapons of Mass Destruction (December 2002)

National Strategy to Secure Cyberspace (February 2003)

Joint National Priorities

National Incident Management System

National Response Plan

National Infrastructure Protection Plan

National Preparedness Goal

Other

NIST Cyber Security Framework

Federal Continuity Directive 1 (FCD 1)

Federal Continuity Directive 2 (FCD 2)

PBS Instructional Letter-PBS-IL-02-1: Implementation of the Interagency Security Committee Security Design Criteria for New Federal Office Buildings and Major Modernization Projects within GSA

NIST 800 53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations

FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors

NOTE: Additional details pertaining to these authorities are available from the SSA upon request.

APPENDIX D

Facility Components and Roles

Facility Component	Examples of Roles
Accounting/Budgeting	Review and prioritize expenditures to ensure adequate funding is available.
Building Services, Public Works	Monitor utility and building automation systems for proper operations and comply with IT and security requirements.
Continuity of Operations Program	Prepare and execute protocols and plans to ensure continuity of essential operations, functions, and services. Periodically review Business Impact Analysis to identify vulnerabilities and understand cascading effects.
Emergency Management Emergency Operations	Prepare for and execute protocols and plans to ensure the safety and security of personnel and property during an emergency.
Human Resources	Ensure that individuals hired receive the proper personnel security reviews appropriate for the security level designated.
Chief Information Officer	Evaluate and assess security requirements for facility information technology systems, identify and implement appropriate countermeasures and monitor performance. Work with CSO in protecting and assessing Building Automation and Physical Security Systems from Cyber Threats.
Intelligence Analysis and Fusion Centers	Review threat information to identify trends and share appropriate information with sector partners.
International Affairs International Relations	Ensure a clear understanding of the threats associated with the political, social, economic, and natural climate so that facility risk can be assessed as needed for overseas facilities.
Law Enforcement Officers	Respond to emergencies, investigate and document suspicious/criminal activity, identify and apprehend offenders. Monitor and support crime reduction through high visibility patrols and operations.
Security Guards	Monitor and control entry posts, screen personnel and packages, and patrol facility interior and perimeter. Should be armed when screening for weapons and meet minimum training requirements. Respond to emergencies, investigate and document suspicious/criminal activity.
Occupational Safety and Health Industrial Safety and Health Radiation Safety	Ensure the safety of individuals in a facility and on surrounding property from a wide variety of hazards, including workplace violence, identified and mitigated as part of facility health and safety assessments. Maintain inventory control of hazardous materials to prevent theft or loss.
Chief Security Officer	Through a Risk Management Process, identify requirements for facility security systems and operations. Implement appropriate countermeasures and assess performance. Work with CIO in protecting and assessing building automation and physical security systems from cyber threats.
Procurement Purchasing Contracting	Ensure that contracts for systems and services include requirements for personnel security, cyber systems security, and built drawings and equipment inventory control. Ensure that contractors meet these requirements. Include facility security requirements in purchase/lease agreements.
Property Management	Conduct pre-purchase/lease review of facility for security considerations. Maintain an inventory of property with appropriate data elements.
Public Affairs Public Relations	Establish and maintain good relations with the community surrounding the facility, including local emergency services. Publicize an appropriate amount of information emphasizing the security of the facility and attention to local issues.
Training Department Exercise Coordinator	Ensure that individuals visiting or working in a facility receive adequate training by the most appropriate means to provide awareness and competencies appropriate for their positions.

APPENDIX E

Coordination and Information Sharing Mechanisms

Committees, Commissions, and Boards	Associations, Councils, and Partnerships	Counterterrorism Focused Task Forces
Interagency Security Committee	NIPP Federal Senior Leadership Council	FBI Insider Threat Task Force
National Security Staff	Federal Real Property Advisory Group	FBI Joint Terrorism Task Forces
National Capitol Region Joint Federal Committee	Federal Facilities Council	Antiterrorism Task Forces
Metropolitan Washington DC Council of Governments System	National Center for Missing and Exploited Children	
Federal Executive Boards	National Crime Prevention Council	
FEMA Regional Interagency Steering Committees	National Governors Association	
Facility Security Committees	American Society for Industrial Security	
	Antiterrorism Advisory Councils	

Information Source Type	Examples
Open Sources of Public Information	<ul style="list-style-type: none"> Newswires, National Newspapers, Radio, Television, Magazines, Internet
Operations and Command Centers	<ul style="list-style-type: none"> Federal: FBI field offices, National Operations Center, National Infrastructure Coordination Center (NICC), National Counterterrorism Center, NORTHCOM FPS MegaCenters, Joint Information Management Center (JIMC), Agency Emergency Operations Centers (EOC's), National Counter Terrorism Center, ICS-CERT State/local: Counterterrorism Intelligence Centers, Synchronized Operations Commands, Terrorism Early Warning Networks, Threat Integration Centers, Fusion Centers
Components of Government at All Levels	<ul style="list-style-type: none"> Federal: Executive, Legislative, and Judicial branches, including departments and agencies State and Local: National Guard; police and sheriff departments; divisions of criminal investigation and intelligence, homeland security, counterterrorism, state attorneys, and public health departments International: Europol, International Criminal Police Organization (Interpol), Canadian Border Intel Center, Australian Crime Commission
Other Information-Sharing and Coordination Mechanisms	<ul style="list-style-type: none"> Homeland Security Information Network (HSIN), Law Enforcement Online (LEO) Regional Information-Sharing System, National Center for Crisis and Continuity Coordination (NC4), Web portals: United States Computer Emergency Response Team (US-CERT), Information Sharing and Analysis Centers (ISAC), Lessons Learned Information Sharing

Sector Coordination and Information Sharing Mechanism	
American Public Works Association	www.apwa.net
American Society for Industrial Security	www.asisonline.org
Annual National Preparedness Report	www.fema.gov/national-preparedness-report
Association of Contingency Planners	www.acp-international.com
Building Owners and Managers International	www.boma.org
Council of State Governments	www.csg.org

Sector Coordination and Information Sharing Mechanism	
Critical Infrastructure Training	www.dhs.gov/critical-infrastructure-training
Critical Infrastructure Partnerships	www.dhs.gov/critical-infrastructure-sector-partnerships
Critical Infrastructure Risk Management Framework	www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience
DHS Daily Open Source Infrastructure Report	https://www.dhs.gov/publication/daily-open-source-infrastructure-report
Emergency Management Assistance Compact	www.emacweb.org
FBI InfraGard	https://www.infragard.org/
Executive Order 13636 (EO-13636)	https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
FBI Joint Terrorism Task Forces	https://www.fbi.gov/about-us/investigate/terrorism/terrorism_itfs
Federal Facilities Council	http://sites.nationalacademies.org/DEPS/FFC/index.htm
Federal Interagency Operational Plans	http://www.fema.gov/federal-interagency-operational-plans
Federal Real Property Association	http://www.frpa.us/
Federal, State, and Major Urban Area Fusions Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers
FPS MegaCenters	http://www.dhs.gov/megacenters
GSA Emergency Operations Center (EOC)	eoc@gsa.gov
Government Forum of Incident Response and Security Teams	www.first.org
General Services Administration Emergency Operations Center	eoc@gsa.gov
Homeland Security Information Network	www.dhs.gov/homeland-security-information-network
Information Sharing and Analysis Centers	www.isaccouncil.org
Information Systems Security Administration	www.issa.org
Institute for Business and Home Safety	www.ibhs.org
Interagency Security Committee	http://www.dhs.gov/interagency-security-committee
International Association of Chiefs of Police	www.theiacp.org
International Association of Fire Chiefs	www.iafc.org
International City/County Management Association	www.icma.org
International Code Council	www.iccsafe.org
International Facility Management Association	www.ifma.org
Lessons Learned for Information Sharing	www.llis.dhs.gov
Major Cities Police Chiefs Association	https://www.majorcitieschiefs.com/
Major County Sheriff's Association	http://www.mcsheriffs.com/
National Association of Counties	www.naco.org
National Center for Crisis and Continuity Coordination	http://www.nc4worldwide.com
National Center for Interstate Compacts	http://www.csq.org/ncic/
National Civic League	http://www.nationalcivicleague.org/
National Conference of State Legislatures	www.ncsl.org
National Congress of American Indians	www.ncai.org
National Council on Readiness and Preparedness	www.ncorp.org
National Counterterrorism Center	www.nctc.gov

Sector Coordination and Information Sharing Mechanism	
National Cybersecurity and Communications Integration Center (NCCIC)	www.dhs.gov/about-national-cybersecurity-communications-integration-center
National Emergency Management Basic Academy	https://training.fema.gov/empp/basic.aspx
National Fire Protection Association	www.nfpa.org
National Governors Association	www.nga.org
National Guard Bureau	http://www.nationalguard.mil
National Incident Management System	https://www.fema.gov/national-incident-management-system
National Infrastructure Coordinating Center (NICC)	www.dhs.gov/national-infrastructure-coordinating-center
National Infrastructure Protection Plan (NIPP)	www.dhs.gov/national-infrastructure-protection-plan
National Institute of Building Science	www.nibs.org
National Joint Terrorism Task Force	https://www.fbi.gov/about-us/investigate/terrorism/terrorism_itfts
National Law Enforcement Telecommunications System	www.nlets.org
National League of Cities	www.nlc.org
National Lieutenant Governors Association	http://www.nlga.us/
National Planning Frameworks and Federal Interagency Operations Plans (IOPs)	www.fema.gov/national-planning-frameworks
National Preparedness Core Capabilities	www.fema.gov/core-capabilities
National Preparedness Goal	www.fema.gov/national-preparedness-goal
National Preparedness System	www.fema.gov/national-preparedness-system
National Property Management Association	www.npma.org
National Safety Council	www.nsc.org
Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)	http://nsi.ncirc.gov/
North East States Emergency Consortium	www.nesec.org
Office of Cyber and Infrastructure Analysis (OCIA)	www.dhs.gov/office-cyber-infrastructure-analysis
Office of Disability Integration and Coordination	https://www.fema.gov/office-disability-integration-and-coordination
Presidential Policy Directive 21 (PPD-21)	https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
Protective Security Advisors (PSAs)	www.dhs.gov/protective-security-advisors
Public-private partnership councils	www.dhs.gov/critical-infrastructure-sector-partnerships
Regional Information Sharing Systems® Program	https://www.riss.net/
Regional Resiliency Assessment Program (RRAP)	www.dhs.gov/regional-resiliency-assessment-program
Responder Knowledge Base (Grants)	http://www.firstresponder.gov/Pages/Responder%20Knowledge%20Base.aspx
Roles, Responsibilities, and Capabilities of Critical Infrastructure Partners and Stakeholders	www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience
Sector Partnership Model	www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience
State Guard Association of the United States	www.sgaus.org
State and Major Urban Area Fusion Centers	https://www.dhs.gov/state-and-major-urban-area-fusion-centers
Strategic National Risk Assessment (SNRA)	www.dhs.gov/strategic-national-risk-assessment-snra
Technical Support Working Group	http://www.cttso.gov/

Sector Coordination and Information Sharing Mechanism	
Threat and Hazard Identification and Risk Assessment (THIRA)	www.fema.gov/threat-and-hazard-identification-and-risk-assessment
United States Computer Emergency Response Team	www.us-cert.gov
U.S. Conference of Mayors	www.usmayors.org

APPENDIX F

SSA and GFS Program Support and Initiatives

This appendix is not inclusive of all programs that are offered across the GFS, but identifies some of the programs that are offered by the SSA and other partners.

	<p>Alarm Monitoring and Dispatch. FPS MegaCenters are the first line of communication disseminating information to law enforcement and then to emergency responders. FPS MegaCenters are high technology alarm monitoring and dispatch control centers that serve as a unique and vital communications link between FPS police officers and contract guards at the entrances to the facilities FPS protects. They monitor all types of alarm systems, closed-circuit televisions, and wireless dispatch communications within Federal facilities to ensure prompt dispatch of law enforcement and emergency first responders to situations at those facilities nationwide. These state-of-the-art communications facilities operate 24 hours a day, 7 days a week.</p>
	<p>Buffer Zone Protection Program (BZPP). DHS BZPP provides targeted grants to increase the general protective capacity and preparedness of local law enforcement and first preventers in communities surrounding facilities. This enhanced protection is intended to make it more difficult for terrorists to conduct planning activities or successfully launch attacks from the immediate vicinity of potential targets. Protection plans complement existing site plans developed for response to terrorist threats or attacks.</p>
	<p>Citizen Corps was created to help coordinate volunteer activities that will make communities safer, stronger, and better prepared to respond to any emergency situation. It provides opportunities for people to participate in a range of measures to make their families, their homes, and their communities safer from the threats of crime, terrorism, and disasters of all kinds. Citizen Corps programs build on the successful efforts that are in place in many communities around the country to prevent crime and respond to emergencies. Programs that started through local innovation are the foundation for Citizen Corps and this national approach to citizen participation in community safety (see www.citizencorps.gov).</p>
	<p>Code Adam Program – National Center for Missing and Exploited Children. The Code Adam program has been a powerful search tool since its beginning in 1994. It is one of the country's largest child safety programs that tries to find lost and possibly abducted children and is advertised in tens of thousands of public and private buildings across the Nation. A Code Adam kit is available to any government facility; the kit includes a training video, poster explaining the program steps, and two decals to put on entrances announcing participation in Code Adam (see www.missingkids.com).</p>
	<p>The Continuity Evaluation Tool (CET) is designed to assess elements of continuity outlined in the annexes of Federal Continuity Directives (FCD) 1 and 2. The purpose of the CET is to evaluate an organization's continuity programs, plans, and procedures. Using the CET to evaluate exercises over multiple years is encouraged to establish a baseline that demonstrates the extent to which organizations have implemented and improved their continuity plans and procedures.</p> <p>There are 14 continuity elements to evaluate within the CET. These 14 continuity elements correspond with 14 of the 17 Annexes found in FCD 1 and the Essential Functions portion of FCD 2. FCD1 Annexes O-Q, (Acronyms, Definitions, and Authorities and References, respectively) do not contain continuity requirements.</p>
	<p>Continuity of Operations (COOP) plans are developed to ensure operations can continue during an incident, and in spite of the aftermath and effects. All Federal executive branch departments and agencies are required by Federal Preparedness Circular 65 to develop, implement, and maintain COOP plans. FEMA's Office of National Security Coordination is the lead agent for these plans (see www.fema.gov/government/coop/index.shtml).</p> <p>COG plans are established to mitigate the consequences of potential natural or manmade catastrophes in situations when the government must continue its essential functions. The importance of government continuity is critical to public confidence in the government's ability to save lives and minimize property loss.</p>
	<p>Contract security guards are often the first line of defense for facilities. They work to protect not only the facility, but also the many people who work in and visit government buildings each day. Contract guards are equipped with countermeasures and the ability to deter, detect, and delay an adversary. In addition to conducting roving patrols of the interior and exterior of Federal facilities, contract security guards provide access control to Federal property through visitor and employee identification checks (e.g., operating security equipment to screen for prohibited items, operating or monitoring security cameras and alarms, and reporting crimes and incidents to the appropriate FPS MegaCenter). Contract security guards also ensure the safety of employees, visitors, and property by maintaining public order and preventing crime. They provide security against loss from mechanical equipment failure or fire, respond to emergency situations involving the safety and security of the facility, act occasionally as a crowd monitor to maintain order, and enforce property rules and regulations.</p>



The Critical Infrastructure Cyber Community (C-Cubed) Voluntary Program, created in February 2014, assists organizations and industries with using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (the Framework) as part of Executive Order 13636: Critical Infrastructure Cybersecurity. The C³ Voluntary Program aims to support critical infrastructure sectors in increasing cyber resilience and to encourage organizations to manage cybersecurity as part of a holistic approach to enterprise risk management.

As part of its goal to encourage organizations to use the Framework, the C³ Voluntary Program conducts three major activities:

- Use: Assist stakeholders with understanding use of the Framework and other risk management efforts, and support development of general and sector-specific use guidance.
- Outreach and Communications: Serve as a point of contact and customer relationship manager to assist organizations with Framework use and guide interested organizations and sectors to DHS and other public and private sector resources to support use of the Framework.
- Feedback: Work with organizations to understand how they are using the Framework, and receive feedback on how the Framework and C³ Voluntary Program resources can be improved to better serve organizations.



Critical Foreign Dependencies Initiative. Through the CFDI, foreign infrastructure that is critical to the Nation is identified, assessed, and prioritized. Sectors and States (particularly border States) have the opportunity to build lists that meet individual risk and incident management needs. The CFDI also provides a forum for the critical infrastructure community to use for the prioritization of critical infrastructure security and resilience during incidents and to enable response and recovery operations.



Cyber Security Evaluation Tool (CSET). FPS Operation Street Talk is an example of an antiterrorism and crime prevention program that features processes for rapid follow-up investigations and information sharing to other echelons of command and other law enforcement agencies as appropriate.



The Design Basis Threat (DBT) Report is a stand-alone threat analysis to be used with the Physical Security Criteria for Federal Facilities: An ISC Standard. The document establishes a profile of the type, composition, and capabilities of adversaries. It is also designed to correlate with the countermeasures in the compendium of standards and to be easily updated as needed.

The DBT is an estimate of the threats that face Federal facilities across a range of undesirable events and based on the best intelligence information, Intelligence Community (IC) reports and assessments, and crime statistics available to the working group at the time of publication. Users of the DBT must consider that undiscovered plots may exist, adversaries are always searching for new methods and tactics to overcome security measures, and the lone-wolf adversary remains largely unpredictable. The intent of the DBT is threefold:

- To inform the deliberations of ISC working groups as they establish standards;
- To support the calculation of risk, based upon threat, vulnerability, and consequences, to a facility when applying ISC's Physical Security Criteria for Federal Facilities; and
- To determine specific adversary characteristics that performance standards and countermeasures are designed to overcome.



The Office of Infrastructure Protection (IP) leads and coordinates national programs and policies on critical infrastructure security and resilience and has established strong partnerships across government and the private sector. The office conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and State, local, tribal, and territorial partners understand and address risks to critical infrastructure. IP provides information on emerging threats and hazards so that appropriate actions can be taken. The office also offers tools and training to partners to help them manage the risks to their assets, systems, and networks.



The DHS Ready Campaign is a national public service advertising campaign produced by the Advertising Council in partnership with DHS. The Ready Campaign is designed to educate and empower Americans to prepare for and respond to emergencies, including natural disasters and potential terrorist attacks (www.ready.gov).



Enhanced Cybersecurity Services (ECS) program is a voluntary information sharing program that assists public and private entities based in the U.S. as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the Federal government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops cyber threat indicators based on this information and shares them with qualified Commercial Service Providers (CSPs), thus enabling them to better protect their customers. ECS augments, but does not replace, entities' existing cybersecurity capabilities.

The ECS program does not involve government monitoring of private networks or communications. Under the ECS program, information relating to threats and malware activities detected by the CSPs is not directly shared between the critical infrastructure CSP customers and the government. However, when a CSP customer voluntarily agrees, the CSP may share limited and anonymized information with ECS.



The **Federal Acquisition Service (FAS)** operates at the core of the GSA mission and supports departments and agencies with resources for Protection, Prevention, Mitigation, Response and Recovery, leveraging the buying power of the Federal government to acquire the best value for taxpayers and Federal, State, local, tribal, and territorial customers. To support the GFS and accomplish its mission, FAS uses innovative techniques and leverages government-wide buying power, acquisition expertise, and electronic tools to successfully deliver new and existing services, products, and solutions.

GSA Schedules are fast, easy, and effective contracting vehicles for both customers and vendors. For GSA Schedules, GSA establishes long-term government-wide contracts with commercial companies to provide access to millions of commercial products and services at volume discount pricing.

Order Products, Supplies, and Services - You can order computers, vehicles, radios, emergency response equipment, and other Infrastructure Protection products, supplies, and services from GSA Schedule contractors or through the GSA Advantage!® online shopping and ordering system.

Value for Customers - Customers contract with pre-approved vendors and benefit from “most-favored customer” pricing with GSA Schedules (also referred to as Multiple Award Schedules (MAS) and Federal Supply Schedules (FSS)). To find out more about GSA Schedules that support Preparedness, Protection, Prevention, Response and Recovery, view our comprehensive GSA Schedules Benefits.



Federal Personnel Security Program. The Office of Personnel Management (OPM) Federal Personnel Security Program ensures the fitness and suitability of applicants for and appointees to positions in the Federal service. To carry out this responsibility, OPM sets government-wide investigations policy for the Federal Personnel Security Program and carries out onsite inspections to ensure that employing agencies are following established policies. Personnel investigations relating to personnel suitability and security also are provided on a reimbursable basis.



Federal Protective Service Facility Security Assessment Program. Through the Facility Security Assessment (FSA) program, FPS accomplishes prioritization on three different levels: facility, regional, and national.

- At the facility level, once the risk has been assessed and the comprehensive report has been prepared and presented to stakeholders, FPS develops countermeasure recommendations that mitigate the vulnerabilities to the selected credible threats. The stakeholder must apply risk management strategies to determine which countermeasures to approve, and to provide funding for implementation. The stakeholder must weigh the risk presented by the FPS Inspector against the availability of resources required to implement the countermeasures. The stakeholder may choose to approve the countermeasures, accept the entire risk, or approve some of the countermeasures and some of the risk.
- At the regional level, credible threats, vulnerabilities, and recommended countermeasures are identified in the field and tracked by FPS. The development, approval, and implementation process for countermeasures in the region are also tracked by FPS; and this information is then used to create threat analysis, trends, and security system requirements throughout the regions.
- At the national level, credible threats, vulnerabilities, and recommended countermeasures are tracked by FPS for the sector. The information is used to aggregate and analyze risk assessment results in order to develop a comprehensive picture of asset, system, and network risk; establish risk-based priorities; and determine protection and business continuity initiatives that provide the greatest risk mitigation across the country.



The **Federal Risk and Authorization Management Program (FedRAMP)** is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Please visit fedramp.gov.



The **GSA Office of Mission Assurance (OMA)** serves as the agency-wide lead for continuity of operations and disaster support policy, planning, and operational coordination. This mission includes:

- Developing structured programs to ensure the resiliency of the GSA emergency functions against the full range of natural and manmade disasters.
- Providing agency leadership with complete situational awareness during crisis operations to allow for an agency-wide and interagency collaborative response to all national disaster operations.

OMA central office and regional staff provides agency-wide leadership and coordination for emergency management and security policy, including occupant emergency planning, response and recovery, personal identity verification, physical security, personnel security, and suitability activities. OMA responsibilities include:

- Continuity of Operations Planning in accordance with the National Continuity Policy and Federal Continuity Directive 1 and 2
- Emergency Support Function 2 and 7 support under the National Response Framework Co lead the Federal Emergency management Agency (FEMA)
- Coordination with FPS to ensure safety and security of GSA owned and leased buildings and building occupants
- Workplace Violence Prevention
- Providing situation awareness and information sharing among Federal, State, local, tribal, and territorial



The **GSA Operations Center (OC)/Emergency Operations Center (EOC)** serves as the agency-wide lead for continuity of operations and disaster support policy, emergency response planning, and operational coordination for over 8,700 GSA owned and leased facilities nationwide. It is a critical asset to the agency and is a vital component of the emergency response process. The EOC is organized to serve as an effective communications center, an information clearinghouse, and an authoritative source for dissemination of information.

For questions, please email EOC@GSA.GOV.



The **Council of State Governments' Healthy States Initiative** is designed to help State leaders make informed decisions on public health issues. The enterprise brings together State legislators, officials from the Centers for Disease Control and Prevention, State health department officials, and public health experts to share information and identify innovative solutions. State legislators play a vital role in determining the structure and resources available to State and local public health agencies. These agencies provide education and interventions across a wide spectrum of public health issues, including emergency preparedness and response

(www.healthystates.csg.org).



Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operators to share sensitive but unclassified information. Federal, state, local, tribal, territorial, international, and private sector homeland security partners use HSIN to manage operations, analyze data, and send alerts and notices. HSIN leverages the trusted identity of its users to provide simplified access to a number of law enforcement, operations, and intelligence information sharing portals. For more information about HSIN, please contact

HSIN.Outreach@hq.dhs.gov.



Identity, Credential and Access Management (ICAM) previously covered under HSPD-12, integrates the management of identity information, credentials, and secure access to buildings, networks, and information technology systems. Through its ICAM efforts, GSA is helping to create a safer, more efficient government.



The **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, State, local, tribal, and territorial governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.



The Science and Technology Directorate (S&T) developed the **Integrated Rapid Visual Screening (IRVS)** methodology for assessing the risk and resilience of all 16 critical infrastructure sectors to terrorist attacks and natural hazards that result in catastrophic losses (fatalities, injuries, damage, or business interruption). The assessment includes terrorist attacks caused by chemical, biological, and radiological (CBR) agents and explosives, and natural disasters resulting from earthquakes, floods, wind, and fire.

The IRVS methodology is often used to obtain a basic understanding of risk and resilience and to prioritize more detailed assessments over the entire inventory of infrastructure considered. Thus, IRVS is intended to be used in a tiered assessment, consisting of successively more refined analyses as more detailed information is provided. The trade-off between level of effort and level of refinement allows an assessment to meet a variety of benefit/cost considerations for different infrastructure.



Interagency Security Committee (ISC). On October 19, 1995, six months after the Oklahoma City bombing of the Alfred P. Murrah Federal Building, President Clinton issued Executive Order 12977, creating the Interagency Security Committee (ISC) to address continuing government-wide security for Federal facilities. Prior to 1995, minimum physical security standards did not exist for nonmilitary Federally owned or leased facilities. The ISC's mandate is to enhance the quality and effectiveness of physical security in and the protection of buildings and nonmilitary Federal facilities in the United States. The ISC standards apply to all nonmilitary Federal facilities in the United States—whether government-owned, leased or managed; to be constructed or modernized; or to be purchased.

Chief security officers and other senior executives from 54 Federal agencies and departments make up the ISC membership. Leadership is provided by the chair, who is the DHS Assistant Secretary for Infrastructure Protection, the Executive Director, and eight standing subcommittees.

The full Interagency Security Committee meets quarterly. Members serve on subcommittees and working groups to develop physical security policies and standards, promote key management practices, and facilitate mitigation of threats to employees and the visiting public. The ISC also engages with industry and other government stakeholders to advance best practices.



Joint Information Management Center (JIMC). Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience reinforces the Federal government's responsibility to protect its own critical infrastructure and mission essential functions, and that proactive and coordinated efforts among all stakeholders are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure. DHS/FPS and GSA, as part of the interagency coordination, have determined that they would create collaborative initiatives and take proactive steps to manage risk and protect critical infrastructure against all hazards that could have debilitating impact on

security, economic stability, and public health and safety. The JIMC effort aims to reduce vulnerabilities, deter threats, minimize consequences, strengthen resilience, and support timely response and recovery decisions and actions for critical infrastructure in the event of a deliberate attack, natural disaster, or other emergency.



The **Level 1 and Level 2 Programs** provide DHS with a means of identifying nationally significant critical assets and systems, and enhance decision-making related to the security and resilience of critical infrastructure. The GFS has actively participated in the DHS Level 1 and Level 2 Program to identify critical facilities for inclusion in the prioritization process. These lists inform the State Homeland Security and other grant programs, and are also used during incidents as a tool for prioritizing Federal, State, and local response and recovery efforts.



FPS uses the Modified Infrastructure Survey Tool (MIST) as part of the FPS FSA process. It is a modified version of the National Protection and Programs Directorate (NPPD) Infrastructure Protection Division (IP), Infrastructure Survey Tool (IST) used by Protective Security Advisors (PSA) and developed by the Argonne National Laboratory. MIST uses a tailored set of questions that helps FPS establish a security baseline and allows for comparison of the facility being surveyed against established security standards. MIST's methodology involves the gathering of data via an assessment question set and processing of that data through an algorithm to convert the data to vulnerability measures.

MIST performs a quantitative analysis of the data for each major countermeasure component and subcomponent that has been entered into the tool and then produces a Protection Measures Index (PMI) for each item and an overall PMI, which is a culmination of all the PMIs. The PMI ranges from 0 (low protection) to 100 (high protection). The PMI has a constructive sense, in that it increases (gets better) as protective measures are added and vulnerabilities are decreased.



The **National Crime Prevention Council's (NCPC)** mission is to be the Nation's leader in helping people keep themselves, their families, and their communities safe from crime. To achieve this, NCPC produces tools that communities can use to learn crime prevention strategies, engage community members, and coordinate with local agencies, including the National Citizens' Crime Prevention Campaign, featuring McGruff the Crime Dog and his slogan, "Take A Bite Out Of Crime" (see www.ncpc.org).



The **National Guard** has a unique dual mission consisting of both Federal and State roles. During peacetime, each State National Guard answers to the leadership in the 50 States, 3 Territories, and the District of Columbia. During national emergencies, however, the President reserves the right to mobilize the National Guard, putting its members on Federal duty status. The National Guard's State mission is perhaps the most visible and well known. Nearly everyone has seen or heard of National Guard units responding to battle fires or helping communities deal with floods, tornadoes, hurricanes, snowstorms, or other emergency situations. In times of civil unrest, the citizens of a State can rest assured that the National Guard will be ready to respond, if needed.



National Critical Infrastructure Prioritization Program (NCIPP). DHS leads the coordination of the national effort to identify and prioritize the security and resilience of the Nation's critical infrastructure through the NCIPP. The NCIPP includes the Level 1 and Level 2 Program, which identifies domestic infrastructure that, if disrupted, could critically impact the Nation's public health and safety, economy, or national security, and the Critical Foreign Dependencies Initiative (CFDI), which identifies similarly critical infrastructure located outside the United States. Other national prioritization programs include facility ranking and mitigation strategies.



The **National Cybersecurity and Communications Integration Center (NCCIC)**, within the Office of Cybersecurity and Communications, serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all Federal departments and agencies; State, local, tribal, and territorial governments; the private sector; and international entities. The center's activities include providing greater understanding of cybersecurity and communications situational awareness, vulnerabilities, intrusions, incidents, mitigation, and recovery actions.



The **National Infrastructure Coordinating Center (NICC)** is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the Federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our Nation's infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets. The NICC is part of the National Protection and Programs Directorate/Office of Infrastructure Protection and the DHS National Operations Center.



National Operations Center (NOC). The Office of Operations Coordination and Planning's (OPS) mission is to integrate DHS and interagency planning and operations coordination in order to prevent, protect, respond to, and recover from terrorist threats/attacks and other manmade or natural disasters. Through the National Operations Center (NOC), DHS OPS interacts with DHS components, State governors, Homeland Security Advisors (HSAs), law enforcement partners, and critical infrastructure operators in all 50 States and more than 50 major urban areas nationwide.

The NOC, using the DHS Common Operating Picture (COP), provides real-time situational awareness and monitoring of the homeland, coordinates incident response activities, issues advisories and bulletins concerning threats to homeland security and provides specific protective measures. The NOC operates 24 hours a day, 365 days a year to coordinate information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents. Information on domestic incident management is shared with EOCs through HSIN.



The **Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)** is a joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and State, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.

The NSI is a standardized process—including stakeholder outreach, privacy protections, training, and facilitation of technology—for identifying and reporting suspicious activity in jurisdictions across the country and also serves as the unified focal point for sharing SAR information.



FPS Operation Street Talk is an example of an antiterrorism and crime prevention program that features processes for rapid follow-up investigations and information sharing to other echelons of command and other law enforcement agencies as appropriate.



Occupant Emergency Plans. Per Title 41 Code of Federal Regulations, Chapter 102-74.230, an OEP is required for all GSA facilities. There should be an OEP for the entire facility, even if each tenant has an individual OEP for their respective space. The ISC Risk Management Process states “the OEP provides direction to the occupants of the building on how to react to emergencies.” At a minimum, the OEP should address:

- Purpose and circumstances for activation;
- Command officials and supporting personnel contact information;
- Occupant life-safety options (e.g., evacuation, shelter-in-place);
- Local law enforcement and first responder response;
- Special needs individuals (e.g., disabled, deaf, etc.);
- Visitors;
- Special facilities (e.g., Sensitive Compartmented Information Facilities (SCIFs), child-care centers);
- Assembly and accountability;
- Security during and after incident; and
- Training and exercises.

The scope and complexity of the OEP is dependent on the facility's size, population, and mission. The OEP must be reviewed annually and updated as appropriate. OEPs must also identify unique planning requirements for staff or functions such as evacuating child-care centers. Users shall document the weakest link when answering this question. In multiple tenant scenarios, this means the agency without a plan will be documented in the structured question sets and all others will have their plans reviewed and documented in the comments section.

Location-specific plans are established that delineate responsibilities and specific procedures to follow in an emergency. Examples include:

- Emergency Action Plans are written documents required by the Occupational Safety and Health Administration (29 CFR 1910.38a) for any workplace where fire extinguishers are required or provided and where individuals would be evacuating during a fire or other emergency. The purpose of an Emergency Action Plan is to facilitate and organize employer and employee actions during workplace emergencies (see <http://osha.gov/SLTC/etools/evacuation/eap.html>).
- Local emergency response plans are prepared in accordance with the provisions of the Emergency Planning and Community Right-to-Know Act. Every community in the United States must be part of a comprehensive emergency response plan. The governor of each State designates a State Emergency Response Commission that is responsible for designating local emergency planning districts and appointed local emergency planning committees for each district that must develop a local emergency response plan, review it at least annually, and provide information about chemicals in the community to citizens.
- Plans typically include procedures for evacuation, shelter in place, medical emergencies, bomb threats, suspicious packages, and natural disasters. Location-specific procedures are added to address unique threats or hazards, such as hazardous materials spills or releases of radioactive materials. Other procedures are generally applicable to all government facilities, such as the Code Adam Program administered by the



PandemicFlu.gov provides comprehensive government-wide information on pandemic influenza and avian influenza for the general public, health and emergency preparedness professionals, policymakers, government and business leaders, school systems, and local communities. It discusses how all parts of the Federal Government are planning and preparing for flu pandemic, as well as information on the integration of Federal, State, and local planning, including flu pandemic summits held in each State (see www.pandemicflu.gov).



Protection of Buildings Located Overseas. Within the Department of State (DOS), Diplomatic Security (DS) has the global responsibility for protecting people, information, and property.

- Regional security officers are assigned to nearly every U.S. diplomatic mission abroad to protect overseas missions from physical and electronic attack.
- Marine Security Guards control access to the interior of missions by monitoring surveillance devices, fire alarms, and communications systems that cover the entire embassy. In times of crisis, they aid in safeguarding the lives of diplomatic personnel and assist in evacuating embassy personnel and other Americans living in the country.
- More than 15,600 local guards, nearly half of whom are devoted to protecting residences, protect the perimeters of overseas missions, office facilities, residences, and construction sites.
- Special agents, in concert with other mission or post elements, formulate plans to deal with various emergency contingencies ranging from hostage taking to evacuations. Since the early 1990s, special agents have worked closely with the military, especially the U.S. Marine Fleet Antiterrorism Security Teams, which have provided emergency force protection support for DOS operations in a number of countries when the host government was unable to do so. Special agents also depend on Marine Security Guards, U.S. Navy Seabees, surveillance detection teams, local guards, cleared American guards, local investigators, host government officials, and other DS elements domestically and abroad to provide assistance in combating criminal, intelligence, and terrorist threats against U.S. interests worldwide.
- Personnel and sensitive information is safeguarded overseas by DS security engineering officers who are responsible for detecting and preventing loss of sensitive information from technical espionage.



GSA Public Building Service (PBS) is the landlord for the civilian Federal government. PBS manages 377 million square feet of workspace for a million Federal employees in 2,100 American communities.

- The Office of Client Solutions is responsible for the coordinating of customer relationships and overseeing service deliveries to GSA customers.
- The Office of Leasing directs the development of procedures and specifications related to realty services and provides advocacy and strategic direction in national GSA real estate issues.
- The Office of Facilities Management and Services Programs provides program management, support, and guidance to Property Managers in an effort to provide a safe, healthy, effective, and efficient work environment for GSA clients.
- The Office of Design and Construction provides national leadership and policy direction in the areas of architecture, engineering, urban development, construction services, and project management.
- The Office of Portfolio Management provides strategic direction, administration, and management support for real estate portfolio management, asset business strategies, capital allocation, portfolio analysis, building operations and maintenance, occupancy administration, and property disposal.



REAL ID is a coordinated effort by the states and the Federal government to improve the reliability and accuracy of state-issued identification documents, which should inhibit terrorists' ability to evade detection by using fraudulent identification. REAL ID implements a 9/11 Commission recommendation urging the Federal government to "set standards for the issuance of sources of identification, such as driver's licenses."

The REAL ID Act of 2005:

- Establishes minimum standards for the production and issuance of state-issued driver's licenses and identification cards, and authorizes grants to assist states in implementing the requirements.
- Prohibits Federal agencies from accepting for official uses driver's licenses and identity cards from States unless the Department of Homeland Security determines that the State meets the standards. Official uses are defined as accessing Federal facilities, entering nuclear power plants, and boarding federally regulated commercial aircraft.
- The ISC issued the "REAL ID Act Implementation: An Interagency Security Committee Guide" in August 2015.



Regional Resiliency Assessment Program Overview (RRAP). The U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) Regional Resiliency Assessment Program (RRAP) is a cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure. Each year, DHS, with input and guidance from Federal and State partners, selects several RRAPs focusing on specific infrastructure sectors within defined geographic areas and addresses all-hazard threats that could result in regionally and/or nationally significant consequences. The RRAP relies on engagement and information sharing with Federal agencies; State, local, tribal, and territorial partners; private sector facility owners and operators; law enforcement; emergency response organizations; academic institutions; and other stakeholders.

During the program's first four years, RRAPs were conducted in most regions of the United States. The projects have focused on sectors, such as Energy, Transportation, Government Facilities, Critical Manufacturing, Commercial Facilities, and Agriculture and Food. The RRAP incorporates vulnerability assessments, capabilities assessments, workshops, and infrastructure protection planning efforts, to assemble an analysis of a region's critical infrastructure and prevention, protection, and resilience capabilities. The RRAP process culminates in a Resiliency Assessment that presents the results and findings of the project, including key resilience gaps and options for resilience enhancements. The Resiliency Assessment, along with supporting documents and content, are provided to select RRAP participants in the form of a Multimedia Presentation. Based on the RRAP series of activities, facility owners and operators and government officials can use RRAP findings and information to make strategic investments in equipment, planning, training, and resources to enhance the security posture of facilities, surrounding communities, and entire regions.



StaySafeOnline – The National Cyber Security Alliance provides cybersecurity awareness and education tools and resources to empower sector partners to stay safe online (see www.staysafeonline.org).



The **Strategic National Risk Assessment (SNRA)** defines numerous threats and hazards to homeland security in the broad categories of adversarial/human-caused, natural, and technological/accidental threats. Critical assets, systems, and networks face many of the threats categorized by the SNRA, including terrorists and other actors seeking to cause harm and disrupt essential services through physical and cyberattacks, severe weather events, pandemic influenza, or other health crises, and the potential for accidents and failures due to infrastructure operating beyond its intended lifespan. The potential for interconnected events with unknown consequences adds uncertainty in addition to the known risks analyzed as part of the SNRA.



The **Threat and Hazard Identification and Risk Assessment (THIRA)** is a common, four-step risk assessment process that helps the whole community—including individuals, businesses, faith-based organizations, nonprofit groups, schools and academia, and all levels of government—understand its risks and estimate capability requirements. The THIRA process helps communities map their risks to the core capabilities, enabling them to determine whole-community informed:

- Desired outcomes;
- Capability targets; and
- Resources required to achieve their capability targets.

The outputs of this process inform a variety of emergency management efforts, including emergency operations planning, mutual aid agreements, and hazard mitigation planning. Ultimately, the THIRA process helps communities answer the following questions:

- What do we need to prepare for?
- What shareable resources are required in order to be prepared?



Training and Exercises. Implementing response plans and procedures requires training and exercises to ensure that facility occupants and local responders know what to do in an actual emergency. The FEMA Emergency Management Institute offers a broad range of training that addresses key elements of the National Incident Management System. The primary purpose of the Integrated Emergency Management curriculum is to teach multiagency coordination.

The Federal Law Enforcement Training Center serves as an interagency law enforcement training organization for more than 80 Federal agencies and provides training to State, local, tribal, and territorial campus law enforcement agencies on a wide range of topics.

The National Exercise Program identifies and integrates national-level exercise activities to ensure those activities serve the broadest community of learning. In addition to full-scale, integrated national-level exercises, it provides tailored exercise activities that serve as DHS' primary vehicle for training national leaders and staff. The National Exercise Program enhances the collaboration among partners at all levels of government for assigned homeland security missions. National-level exercises provide the means to conduct full-scale, full-system tests of collective preparedness, interoperability, and collaboration across all levels of government and the private sector. The program also incorporates elements to allow us to identify the implications of changes to homeland security strategies, plans, technologies, policies, and procedures.



United States Computer Emergency Readiness Team (US-CERT). The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity—collaborative, agile, and responsive in a dynamic and complex environment.

APPENDIX G

Continuity

Continuity of Operations, as defined in the National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20) and the National Continuity Policy Implementation Plan (NCPIP), is an effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

The Goal of Continuity

The ultimate goal of continuity in the Executive branch is the continuation of National Essential Functions (NEFs). In order to achieve that goal, the objective for organizations is to identify their Essential Functions (EFs) and ensure that those functions can be continued throughout or resumed rapidly after a disruption of normal activities. The Federal Government has an important partnership with other non-Federal government entities and with private sector owners and operators who play integral roles in ensuring our homeland security.

Continuity Program Management Cycle

An organization's resiliency is directly related to the effectiveness of its continuity capability. An organization's continuity capability—its ability to perform its essential functions continuously—rests upon key components or pillars, which are in turn built on the foundation of continuity planning and program management. Those key pillars are Leadership, Staff, Communications, and Facilities. The continuity program staff within an agency shall coordinate and oversee the development and implementation of continuity plans and supporting procedures.

A standardized continuity program management cycle ensures consistency across all continuity programs and supports the foundation and pillars that comprise the Nation's continuity capability. It establishes consistent performance metrics, prioritizes implementation plans, promulgates best practices, and facilitates consistent cross-agency continuity evaluations.



Description of Functions

The identification and prioritization of essential functions are a prerequisite for continuity planning because they establish the planning parameters that drive an organization's efforts in all other planning and preparedness areas. These functions are activities that are conducted to accomplish an organization's mission and serve its stakeholders. During an event that necessitates the activation of continuity plans, the resources and staff available to an organization will likely be limited, and the organization will not be able to perform all of its normal functions. Therefore, a subset of those functions that are determined to be critical activities are defined as the organization's essential functions. These essential functions are used to identify supporting tasks and resources that must be included in the organization's continuity planning process.

Continuity Partners

NSPD-51/HSPD-20, National Continuity Policy, recognizes the importance of partnerships and interrelationships and specifically notes "Federal Government COOP ... shall be appropriately integrated with ... State, local, tribal, and territorial governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to promote interoperability and to prevent redundancies and conflicting lines of authority." Additionally, the policy encourages "the integration of Federal continuity plans and operations with State, local, tribal, and territorial governments,

and private sector owners and operators of critical infrastructure, as appropriate, in order to provide for the delivery of essential services during an emergency."

Continuity cannot occur without the commitment and dedication of many partners who play integral roles in ensuring homeland security and providing critical functions and services to the Nation’s citizens. Independent government entities at all levels and individual private sector companies are intimately connected and work together in critical partnership to ensure continuation of essential functions. As part of each organization’s continuity planning and identification of its essential functions, it is critical that each organization clearly identify its partners and, in particular, those supplies, products, information, and other inputs the organization receives from partners that are vital to the organization’s ability to accomplish its essential functions.

National Essential Functions (NEFs)

At the Federal level, the NSPD-51/HSPD-20, National Continuity Policy, Federal Continuity Directive 1 (FCD 1), and Federal Continuity Directive 2 (FCD 2) establish and detail NEFs, Primary Mission Essential Functions (PMEFs), Mission Essential Functions (MEFs), and Essential Supporting Activities (ESAs).

ESFs and Primary and Secondary agencies for all ESFs

The ESFs provide the structure for coordinating Federal interagency support for a Federal response to an incident. They are mechanisms for grouping functions most frequently used to provide Federal support to States and Federal-to-Federal support, both for declared disasters and emergencies under the Stafford Act and other non-Stafford Act emergencies.

The Incident Command System provides for the flexibility to assign ESF and other stakeholder resources according to their capabilities, taskings, and requirements to augment and support the other sections of the Joint Field Office (JFO)/Regional Response Coordination Center (RRCC) or National Response Coordination Center (NRCC) in order to respond to incidents in a more collaborative and cross-cutting manner.

While ESFs are typically assigned to a specific section at the NRCC or in the JFO/RRCC for management purposes, resources may be assigned anywhere within the Unified Coordination structure. Regardless of the section in which an ESF may reside, that entity works in conjunction with other JFO sections to ensure that appropriate planning and execution of missions occur.

Primary Agencies

An ESF primary agency is a Federal agency with significant authorities, roles, resources, or capabilities for a particular function within an ESF. ESFs may have multiple primary agencies, and the specific responsibilities of those agencies are articulated within the relevant ESF Annex. A Federal agency designated as an ESF primary agency serves as a Federal executive agent under the Federal Coordinating Officer (or Federal Resource Coordinator for non-Stafford Act incidents) to accomplish the ESF mission.

Support Agencies

Support agencies are those entities with specific capabilities or resources that support the primary agency in executing the mission of the ESF.

Continuity Community and Sector-Specific Agency Overlap

There are 16 critical infrastructure sectors and 15 Emergency Support Functions. There is no overlap between the SSAs and EFSs, but they support each other. If you take a holistic approach in looking at the role of each conclave, they support the five national preparedness mission areas of prevention, protection, mitigation, response, and recovery. The sectors address prevention, protection and deterrence; when an event occurs, the ESFs address mitigation, response, and recovery.

ESF & Lead Agency	Sector & SSA	ESF Scope
-------------------	--------------	-----------

ESF & Lead Agency	Sector & SSA	ESF Scope
ESF #1 – Transportation Lead Agency – DOT	Transportation SSA – DHS/DOT	<ul style="list-style-type: none"> • Aviation/airspace and control • Restoration/recovery of transportation infrastructure • Transportation safety • Movement restrictions • Damage and impact assessment
ESF #2 – Communications Lead Agency – DHS/NCS, DHS FEMA	Communications and Information Technology SSA – DHS	<ul style="list-style-type: none"> • Coordination with telecommunications and information technology industries • Protection, restoration, and sustainment of national cyber and information technology resources • Restoration and repair of telecommunications infrastructure • Oversight of communications within the Federal incident management and response structure
ESF #3 – Public Works and Engineering Lead Agency – DOD/USACE, DHS/FEMA	Sector: Emergency Services and Transportation SSA – DHS/DOT	<ul style="list-style-type: none"> • Infrastructure protection and emergency repair • Engineering services and construction management • Infrastructure restoration • Emergency contracting support for life-saving services
ESF #4 – Firefighting Lead Agency – USDA/FS	Sector: Emergency Services SSA – Federal/SLTT Emergency Services	<ul style="list-style-type: none"> • Coordination of Federal firefighting activities • Support to wildland, rural, and urban firefighting operations
ESF #5 – Emergency Management Lead Agency – DHS/FEMA	All	<ul style="list-style-type: none"> • Coordination of incident management and response efforts • Resource and human capital • Financial management • Issuance of mission assignments • Incident action planning
ESF #6 – Mass Care, Emergency Assistance, Housing, and Human Services Lead Agency – DHS/FEMA	Sector: Healthcare and Public Health SSA – HHS/Federal, SLTT Emergency Services	<ul style="list-style-type: none"> • Mass care • Disaster housing • Emergency assistance • Human services
ESF #7 – Logistics Management and Resource Support Lead Agency – FEMA, GSA	Sector: Commercial Facilities/Critical Manufacturing/Defense Industrial Base SSA – DHS/DOD	<ul style="list-style-type: none"> • Comprehensive, national incident logistics planning, management, and sustainment capability • Resource support (e.g., facility space, office equipment and supplies, contracting services, etc.)
ESF#8 – Public Health and Medical Services Lead Agency – HHS	Sector: Emergency Services SSA – HHS/Federal, SLTT Emergency Services	<ul style="list-style-type: none"> • Public health • Mental health services • Medical • Mass fatality management
ESF# 9 – Search and Rescue Lead Agency – DOD, DHS/FEMA, DHS USCG, DOI	Sector: Emergency Services SSA – DHS/Federal, SLTT Emergency Services	<ul style="list-style-type: none"> • Life-saving assistance • Search and rescue operations
ESF# 10 – Oil and Hazardous Materials Response Lead Agency – DHS/USCG, EPA	Sector: Energy Sector SSA – DOE	<ul style="list-style-type: none"> • Oil and hazardous materials (chemical, biological, radiological, etc.) • Environmental short and long term cleanup
ESF# 11 – Agriculture and Natural	Sector: Food and Agriculture	<ul style="list-style-type: none"> • Nutrition assistance

ESF & Lead Agency	Sector & SSA	ESF Scope
Resources Lead Agency – USDA, DOI	SSA – USDA/HHS	<ul style="list-style-type: none"> • Food safety and security • Safety and well-being of household pets • Animal and plant disease and pest response • Natural and cultural resources and historic properties protection and restoration
ESF# 12 – Energy Lead Agency – DOC	Sector: Energy/ Nuclear/ Water/ Dams SSA – DHS/DOE	<ul style="list-style-type: none"> • Energy infrastructure assessment, repair, and restoration • Energy forecast • Energy industry utilities coordination
ESF# 13 – Public Safety and Security Lead Agency – DOJ	Sector: Government Facilities/ Emergency Services SSA – DHS FPS-GSA/ Federal, SLTT Emergency Services	<ul style="list-style-type: none"> • Facility and resource security • Public safety and security support • Security planning and technical resource assistance • Support to access, traffic, and crowd control
ESF# 14 – Long-Term Community Recovery Lead Agency – USDA, DHS, DHS/FEMA, HUD, SBA	Sector: All Sectors SSA – All SSAs	<ul style="list-style-type: none"> • Social and economic community impact assessment • Analysis and review of mitigation program implementation • Long-term community recovery assistance to States, local governments, and the private sector
ESF# 15 – External Affairs Lead Agency – All Gov’t agencies	Sector: All Sectors SSA – All	<ul style="list-style-type: none"> • Emergency public information and protection action guidance • Congressional and international affairs • Media and community relations • Tribal and insular affairs