Financial Services Sector-Specific Plan 2015

This page intentionally left blank.

Financial Services Sector-Specific Plan

2015

Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Financial and Banking Information Infrastructure Committee
FBIIC

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

Introductory Comments

We are pleased to present the 2015 Financial Services Sector-Specific Plan (SSP) which provides an overview of the sector and the cybersecurity and physical risks it faces, establishes a strategic framework that serves as a guide for prioritizing the sector's day-to-day work, and describes the key mechanisms through which this strategic framework is implemented and assessed. This plan was developed through close collaboration among the U.S. Department of the Treasury (Treasury), the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), the Financial and Banking Information Infrastructure Committee (FBIIC), and the U.S. Department of Homeland Security. Collectively, this plan reflects the efforts of hundreds of public and private sector stakeholders representing all aspects of the sector.

The organizations that make up the Financial Services Sector form the backbone of the Nation's financial system and are a vital component of the global economy. These organizations are tied together through a network of electronic systems with innumerable entry points. An incident, whether manmade or natural, impacting these systems could have detrimental effects on the entire economy. Our SSP provides a shared strategy for reducing the risk associated with such an event. As an element of the 2013 National Infrastructure Protection Plan (NIPP) framework, this plan enables integration of the Financial Services Sector's security and resilience efforts with the broader national framework of critical infrastructure protection activities.

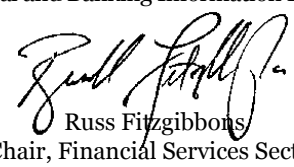
This SSP responds to the evolving risk environment, especially the increasing importance of cybersecurity to the sector, and reflects progress made on building a collaborative public-private partnership since the release of the 2010 SSP. Examples of Financial Services Sector accomplishments since publication of the 2010 SSP include:

- Creating a public-private cybersecurity exercise program to test and improve incident response processes;
- Significantly expanding the sector's cybersecurity information sharing capabilities, including through the rapid growth of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the establishment of Treasury's Financial Sector Cyber Intelligence Group (CIG);
- Establishing a formalized structure of joint working groups to advance specific tasks;
- Formalizing processes for coordinating technical assistance activities; and
- Expanding collaboration with cross-sector and international partners.

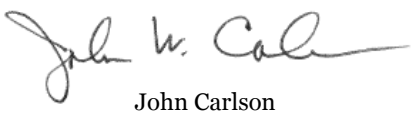
The Financial Services Sector private and public sector coordinating councils – the FSSCC and FBIIC respectively – are pleased to support this SSP and look forward to sustaining and enhancing the security and resilience of critical infrastructure in the sector.

Amias Gerety
Acting Assistant Secretary, Financial Institutions
U.S. Department of the Treasury
Chair, Financial and Banking Information Infrastructure Committee

Caitlin Durkovich
Assistant Secretary, Infrastructure Protection
U.S. Department of Homeland Security



Russ Fitzgibbons
Chair, Financial Services Sector
Coordinating Council



John Carlson
Vice Chair, Financial Services Sector
Coordinating Council

This page intentionally left blank.

Executive Summary

The security and resilience of the Financial Services Sector depends on close collaboration among a broad set of partners, including Financial Services Sector companies; sector trade associations; Federal government agencies; financial regulators; State, local, tribal, and territorial governments; and other government and private sector partners in the U.S. and around the world. These partners seek to reduce the physical and cybersecurity risks that take many forms but, particularly in the case of cybersecurity threats, are becoming increasingly pressing.

Responding to a broad set of risks in a complex environment requires a shared and flexible strategic framework to inform decision-making among individual stakeholders, each of whom maintains their own distinct approach to risk management. The 2015 SSP provides an overview of the sector and the risk it faces, establishes a strategic framework that serves as a guide for prioritizing the sector's day-to-day work, and describes the key mechanisms through which the strategic framework is implemented and assessed.

The Financial Services Sector pursues a shared security and reliance mission:

Continuously enhance security and resilience within the Financial Services Sector through a strong community of private companies, government agencies, and international partners that establishes shared awareness of threats and vulnerabilities, continuously enhances baseline security levels, and coordinates rapid response to and recovery from significant incidents as they occur.

Executing this mission and working to achieve the sector's goals and priorities advances a shared security and resilience vision:

A secure and stable financial system operating environment that maintains confidence in the integrity of global financial transactions, assets, and data.

In order to improve its security and resilience and advance its vision and mission, the sector works to advance four primary goals:

1. Implement and maintain structured routines for sharing timely and actionable information related to cybersecurity and physical threats and vulnerabilities among firms, across sectors of industry, and between the private sector and government.

2. Improve risk management capabilities and the security posture of firms across the Financial Services Sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.

3. Collaborate with the homeland security, law enforcement, and intelligence communities; financial regulatory authorities; other sectors of industry; and international partners to respond to and recover from significant incidents.

4. Discuss policy and regulatory initiatives that advance infrastructure security and resilience priorities through robust coordination between government and industry.

Each goal is, in turn, accomplished through work done on a set of shared sector priorities that help to guide day-to-day work in a manner consistent with the NIPP's goals and the joint national priorities, and in support of a whole-of-nation effort to improve security and resilience across sectors.

Introduction

The Financial Services Sector faces a complex and evolving risk environment that has the potential to disrupt the sector's ability to deliver services that are critical to the nation's economy. To manage this risk, a diverse set of stakeholders—including Financial Services Sector companies; sector trade associations; Federal government agencies; financial regulators; State, local, tribal, and territorial governments; and other government and private sector partners in the United States and around the world—collaborate to enhance the sector's security and resilience.

The 2015 SSP provides an overview of the sector and the risk it faces, establishes a strategic framework that serves as a guide for prioritizing the sector's day-to-day work, and describes the key mechanisms through which the strategic framework is implemented and assessed. To ensure consistency with other national security and resilience efforts, the SSP aligns to the priorities set forth in the 2013 NIPP and the joint national priorities, which provide a common national focal point for partnership efforts across sectors, as demonstrated in Appendix A.

The SSP is a product of the ongoing collaboration on Financial Services Sector security and resilience issues among public and private sector partners, who have a long history of identifying and achieving shared goals and priorities to reduce risk. This SSP also responds to the evolving risk environment, especially the increasing importance of cybersecurity to the sector, and reflects progress made on building a collaborative public-private partnership since the release of the 2010 SSP.

Sector Overview

The Financial Services Sector is highly diverse. Each financial institution has unique security and resilience needs, resources, and plans depending on the functions it performs and its approach to risk management.

Effectively reducing the sector's physical and cybersecurity risk requires a shared understanding of the critical services the sector provides, the specific security and resilience risks it faces, and the collaboration mechanisms used among the sector's security and resilience stakeholders.

Sector Profile

The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities.

Financial institutions are organized and regulated based on the services the institutions provide. Therefore, the profile of the sector is best described by defining the services offered. These categories include: (1) deposit, consumer credit, and payment systems products; (2) credit and liquidity products; (3) investment products; and (4) risk transfer products.

Deposit, Consumer Credit, and Payment Systems Products

Depository institutions of all types are the primary providers of wholesale and retail payments services, such as wire transfers, checking accounts, and credit and debit cards. Depository institutions and their technology service providers facilitate the conduct of transactions across the payments infrastructure, including electronic large value transfer systems, automated clearinghouses (ACH), and automated teller machines (ATM). These institutions are the primary point of contact with the sector for many individual customers.

In addition, depository institutions provide customers with various forms of extensions of credit, such as mortgages and home equity loans, collateralized and uncollateralized loans, and lines of credit, including credit cards. Consumers have multiple ways of accessing these services. For example, customers can make deposits in person at a depository institution's branch office, over the Internet, at an ATM, through the mail, via direct deposit using ACH transactions, via remote deposit capture, or on mobile devices.

These institutions may be National or State-chartered banks or credit unions. At the Federal level, primary regulatory responsibility for depository institutions is carried out by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC). In addition, the Consumer Financial Protection Bureau (CFPB) has responsibility for consumer protection laws. These regulators, along with the State Liaison Committee, develop uniform principles, guidances, and forms through the Federal Financial

Institution Examination Council (FFIEC). In addition, State agencies regulate institutions that are State-chartered according to their authorities.

Credit and Liquidity Products

Customers seek liquidity and credit for a wide variety of needs. For example, individuals may seek a mortgage to purchase a home, businesses may obtain a line of credit to expand their operations, and governments may issue sovereign debt obligations to fund operations or manage monetary and economic policy. Many financial institutions, such as depository institutions, finance and lending firms, securities firms, and government sponsored enterprises (GSEs) meet customers' long- and short-term needs through a variety of financial products. Some of these entities provide credit directly to the end customer, while others do so indirectly by providing liquidity to those financial services firms that provide these services on a retail basis.

Essential to the credit and liquidity markets is the assurance that these products are available with integrity, fairness, and efficiency. The law provides consumer protections, including against fraud involving these products. Furthermore, credit and liquidity products are governed by a complex body of laws. These laws include Federal and State securities laws, banking laws, and laws that are tailored to the specifics of a particular class of lending activity.

Investment Products

Diversity of investment service providers and products promotes the global competitiveness of U.S. financial markets. These products provide opportunities for both short- and long-term investments and include debt securities (such as bonds and bond mutual funds), equities (such as stocks or stock mutual funds), exchange-traded funds, and derivatives (such as options and futures). Securities firms, depository institutions, pension funds, and GSEs all offer financial products that are used for investing needs. These investment products are issued and traded in various organized markets, from physical trading floors to electronic markets. The Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), banking regulators, and insurance regulators all provide financial regulation for certain investment products, along with self-regulatory organizations.

Risk Transfer Products (Including Insurance)

The transfer of financial risks, such as the financial loss due to theft or the destruction of physical or electronic property resulting from a fire, cybersecurity incident, or other loss event, or the loss of income due to a death or disability in a family, is an important tool for the sustainability of businesses and economic vitality of individuals and their families. A wide variety of financial institutions provide risk transfer products to meet this market need.

The U.S. market for financial risk transfer products is among the largest in the world, measuring in the trillions of dollars. These products range from being noncomplex to highly complex. For example, insurance companies, futures firms, and forward market participants offer financial products that allow customers to transfer various types of financial risks under a myriad of circumstances. Market participants often engage in both financial investments as well as in financial risk transfers that enable risk hedging. Financial derivatives, including futures and security derivatives, can provide both of these functions for market participants.

Sector Risks

Financial institutions face an evolving and dynamic set of risks, including operational, liquidity, credit, legal, and reputational risk. The SSP focuses specifically on a subset of operational risk factors against which capital cannot be held that include managing the possibility of a physical or cybersecurity incident that jeopardizes critical systems.

Collectively, these organizations form the backbone of the Nation's financial system and are a vital component of the global economy. These organizations are tied together through a network of electronic systems with innumerable entry points. An incident, whether manmade or natural, impacting these systems could have detrimental impacts throughout the economy.

Most of the sector's key services are provided through or conducted on information and communications technology platforms, making cybersecurity especially important to the sector. Malicious cyber actors continue to target the Financial Services Sector. These actors vary considerably in terms of motivation and capability, but all cybersecurity incidents, regardless of the original motive, have the potential to disrupt critical systems, even inadvertently.

In addition, the sector faces ongoing risks associated with natural disasters, as well as the potential for physical attacks. Hurricanes, tornadoes, floods, and terrorist attacks all have the potential to cause physical disruptions that have significant impacts on Financial Services Sector operations.

- The attacks of September 11, 2001, caused the securities markets and several futures exchanges to close until communications and other services were transferred to alternate sites or restored to lower Manhattan.

- Beginning in the summer of 2012, financial institutions, including smaller institutions, experienced a series of coordinated distributed denial-of-service (DDoS) attacks against their public-facing websites. These incidents affected customer access to banking information, but did not impact core systems or processes.

- On October 29, 2012, the landfall of Superstorm Sandy caused a two-day closure of major equities exchanges, while fixed income markets were closed for one day.

- In recent years, cybercriminals have accessed numerous retailer and other networks to steal credit card information and other financial data.

To reduce the risk associated with incidents like these, the Financial Services Sector continuously assesses its risk posture by understanding its vulnerabilities and the current threat landscape and adjusting its approach to security and resilience based on these assessments. Risk assessments are a long-standing and accepted practice within the Financial Services Sector and are widely conducted by individual institutions and expected by regulators.

To aid in assessing the risk to the sector overall, U.S. Department of the Treasury (Treasury), financial regulators, the U.S. Department of Homeland Security (DHS), law enforcement and other government partners regularly coordinate with financial institutions to share information

about current and emerging threats, develop mitigation strategies, and determine whether any existing or new assets or processes may be critical to the operations of the sector and, thus, require special attention. This coordination occurs primarily through the exchange of incident data, through the collaborative development of threat and mitigation information products, and regularly scheduled and event-driven meetings, as well as through regulatory processes.

Essential to understanding the sector's cybersecurity and physical risks is the identification of critical processes and their dependence on information technology and supporting operations for the delivery of financial products and services. As the sector integrates new information and communications technologies to meet market demand for more efficiency and innovative services, new risks may emerge. Given that financial institutions and technology service providers are tightly interconnected in a dynamic marketplace, an incident impacting one firm has the potential to have cascading impacts that quickly affect other firms or sectors. This risk is exacerbated by the fact that financial institutions depend on other sectors for key services like electricity, communications, and transportation.

In order to manage risk most effectively, many institutions work to identify infrastructure and processes that are most sensitive and take extra precautions to protect that infrastructure. At the same time, identifying the institutions that perform critical operational roles for the sector is key to assuring their rapid recovery from a disruption of their critical functions, regardless of the cause. Identifying key infrastructure, processes, and institutions is also necessary for developing appropriate business continuity planning and recovery protocols as well as continually testing and refining those protocols.

As appropriate, financial institutions, executive branch agencies, financial regulators, and others work together to document critical systems, infrastructure, and institutions and use that information to inform security and resilience programs. For example, Section 9 of Executive Order (EO) 13636 requires that DHS identify critical infrastructure against which a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security. The primary purpose of this process is to better understand national and regional cyber dependencies and consequences across critical infrastructure, inform planning and program development for Federal critical infrastructure security and resilience programs, and motivate identified critical infrastructure owners and operators to maintain robust cyber risk management programs.

Under the EO 13636 Section 9 framework, owners and operators of identified critical infrastructure whose business and operations depend on an extensive network of information and communications technology and software (or "cyber dependent") may be eligible for expedited processing of clearance through the DHS Private Sector Clearance Program, which may provide access to classified government cybersecurity threat information as appropriate. Cyber-dependent critical infrastructure may also be prioritized for routine and incident-driven cyber technical assistance activities offered by DHS and other agencies. As Federal government resources and programs develop and improve to enhance the security and resilience of critical infrastructure against cybersecurity threats, cyber-dependent critical infrastructure will be a continued priority.

Critical Infrastructure Partners

In response to the cybersecurity and physical risks faced by the sector, a network of Financial Services Sector companies; sector trade associations; Federal government agencies; financial regulators; State, local, tribal, and territorial governments; and other government and private sector partners in the U.S. and around the world collaborate on multiple levels to enable the sector's security and resilience. These partnerships are at times formal and at other times more informal.

The Financial Services Sector's umbrella organizations for critical infrastructure protection are the private-sector-led Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and the government-led Financial and Banking Information Infrastructure Committee (FBIIC). The FSSCC and FBIIC respectively serve as the Sector Coordinating Council and Government Coordinating Council for the Financial Services Sector. The FBIIC and FSSCC collaborate closely, including through triannual joint meetings, based on the structure established in Presidential Policy Directive 21 (2014) and the NIPP.

The Financial Services Sector critical infrastructure partnership includes a variety of stakeholders in addition to the FSSCC and FBIIC:

- Private Sector: FSSCC, Financial Services Information Sharing and Analysis Center (FS-ISAC), individual firms, trade associations, regional coalitions, security service providers, technology service providers, and industry partners from other sectors;
- Executive Branch: Treasury, DHS (including the United States Secret Service), U.S. Department of Justice (including the Federal Bureau of Investigation), U.S. Department of Defense, and other departments and agencies;
- Financial Regulators: FBIIC agencies,[1] which includes banking and credit union regulators; securities regulators; self-regulatory organizations; and State regulators;
- State, Local, Tribal, and Territorial Partners; and
- International: Non-U.S. based financial institutions and service providers, non-U.S. regulators, and non-U.S. law enforcement, intelligence community, and homeland security government partners.

It is important to emphasize that financial institutions provide services under the supervision of a well-established regulatory framework. The U.S. financial regulatory system includes both Federal and State regulatory agencies and, in some cases, self-regulatory organizations. Among their responsibilities, regulatory agencies are concerned with institutional and systemic ability

1 American Council of State Savings Supervisors, Commodity Futures Trading Commission, Conference of State Bank Supervisors, Consumer Financial Protection Bureau, Department of the Treasury, Farm Credit Administration, Federal Deposit Insurance Corporation, Federal Housing Finance Agency, Federal Reserve Bank of Chicago, Federal Reserve Bank of New York, Board of Governors of the Federal Reserve System, National Association of Insurance Commissioners, National Association of State Credit Union Supervisors, National Credit Union Administration, North American Securities Administrators Association, Office of the Comptroller of the Currency, Securities and Exchange Commission, and Securities Investor Protection Corporation

to withstand operational disruptions and strive to promote confidence in the Financial Services Sector.

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security Structure

The FSSCC serves as the Sector Coordinating Council for the Financial Services Sector. As of December 2015, the FSSCC membership involves 24 sector associations and 46 financial institutions representing major subsectors of the industry. Specifically, trade groups, such as the American Bankers Association, the Financial Services Roundtable, The Clearing House, the Securities Industry and Financial Markets Association, NACHA, Independent Community Bankers of America, and the Bank Administration Institute, participate actively in the FSSCC and play a strong role in supporting collaborative efforts among their members and with other groups. Furthermore, regional coalitions like ChicagoFIRST play a critical role in coordinating security and resilience efforts among financial institutions spread throughout the nation.

The FSSCC and its member organizations promote security and resilience of the sector through information sharing, incident response, and recovery efforts, and by promoting best practices and the development of effective policies. In addition, the FS-ISAC, which serves as the operational arm of the FSSCC, shares specific information pertaining to cybersecurity and physical risks and distributes recommendations for protective measures and practices to thousands of institutions across the sector.

Financial and Banking Information Infrastructure Committee Structure

The FBIIC serves as the Government Coordinating Council for the Financial Services Sector. The Financial Services Sector is highly regulated by authorities that provide oversight and guidance and examine the financial institutions within their statutory purview. The financial regulators work together along with Treasury through the FBIIC to coordinate efforts with respect to critical infrastructure resilience issues, including efforts related to information sharing, best practices, and incident response.

In addition to monthly meetings among FBIIC staff, agency heads and other senior officials from FBIIC member agencies meet on a regular schedule to provide strategic and policy guidance to the FBIIC; ensure continued senior-level engagement on, and resourcing of, infrastructure protection issues; and enhance the processes for rapidly coordinating significant issues at the most senior levels of government.

FBIIC also collaborates closely in its work with Federal Executive Branch agencies, especially with the DHS and the United States Secret Service, the U.S. Department of Justice and the Federal Bureau of Investigation, and the U.S. Department of Defense. These agencies provide critical assistance to the Financial Services Sector by sharing information about cybersecurity and physical risks, supporting and leading incident response and investigation efforts, and developing and sharing best practice recommendations. The sector has also benefited from close collaboration with the National Institute of Standards and Technology (NIST) on the development of the NIST Cybersecurity Framework.

Treasury's Office of Critical Infrastructure and Compliance Policy (OCIP), which is not a regulator, is responsible for carrying out the Department's duties as the Sector-Specific Agency (SSA) for the Financial Services Sector. As the SSA, Treasury is responsible for providing institutional knowledge and specialized expertise related to the Financial Services Sector as well as leading, facilitating, or supporting the security and resilience programs and associated activities in the all-hazards environment.[2] This work includes serving as the chair of the FBIIC.

Collaboration

Effectively responding to the cybersecurity and physical risks facing the Financial Services Sector requires close collaboration between a host of public and private entities. To advance this collaboration, the FSSCC and FBIIC work closely together on specific projects based on the strategic framework outlined below. This work often occurs through collaborative working groups designed to ensure that the right expertise is brought to bear on key problems.

2 Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274

Strategic Framework

Responding to a broad set of risks in a complex environment requires a shared and flexible strategic framework to inform decision-making among individual stakeholders, each of whom maintains their own distinct approach to managing risk. The need for a shared strategy is especially important in the Financial Services Sector, where tightly interconnected companies must work closely together along with government to improve security and resilience. This SSP serves as a guide for future collaboration by defining a shared strategic framework that consists of the sector's mission, vision, goals, and priorities.

The Financial Services Sector pursues a shared security and reliance mission:

Continuously enhance security and resilience within the Financial Services Sector through a strong community of private companies, government agencies, and international partners that establishes shared awareness of threats and vulnerabilities, continuously enhances baseline security levels, and coordinates rapid response to and recovery from significant incidents as they occur.

Executing this mission and working to achieve the sector's goals and priorities advances a shared security and resilience vision:

A secure and stable financial system operating environment that maintains confidence in the integrity of global financial transactions, assets, and data.

In order to improve its security and resilience, the sector works to advance four primary goals, which provide a framework for identifying and prioritizing collaborative programs and initiatives, especially among the FBIIC and FSSCC:

1. Implement and maintain structured routines for sharing timely and actionable information related to cybersecurity and physical threats and vulnerabilities among firms, across sectors of industry, and between the private sector and government.

2. Improve risk management capabilities and the security posture of firms across the Financial Services Sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.

3. Collaborate with the homeland security, law enforcement, and intelligence communities; financial regulatory authorities; other sectors of industry; and international partners to respond to and recover from significant incidents.

4. Discuss policy and regulatory initiatives that advance infrastructure security and resilience priorities through robust coordination between government and industry.

Each goal is, in turn, accomplished through work done to advance a set of shared sector priorities, which help to guide day-to-day work. Taken together, this strategic framework aligns to the NIPP priorities and the joint national priorities, supporting whole-of-nation efforts to improve security and resilience across sectors.

Information Sharing	
GOAL 1	*Implement and maintain structured routines for sharing timely and actionable information related to cybersecurity and physical threats and vulnerabilities among firms, across sectors of industry, and between the private sector and government.*
PRIORITY	1. Improve the timeliness, quality, and reach of threat and trend information shared within the sector, across sectors, and between the sector and government. 2. Address interdependencies by expanding information sharing with other sectors of critical infrastructure and international partners. 3. Accelerate the sharing of information through structured information sharing processes and routines.

Best Practices	
GOAL 2	*Improve risk management capabilities and the security posture of firms across the Financial Services Sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.*
PRIORITY	1. Promote sector-wide usage of the NIST Cybersecurity Framework, including among smaller and medium sized institutions. 2. Encourage the development and use of best practices for managing third-party risk.

Incident Response and Recovery	
GOAL 3	*Collaborate with the homeland security, law enforcement, and intelligence communities; financial regulatory authorities; other sectors of industry; and international partners to respond to and recover from significant incidents.*
PRIORITY	1. Streamline, socialize, and enhance the mechanisms and processes for responding to incidents that require a coordinated response. 2. Routinely exercise government and private sector incident response processes.

Policy Support	
GOAL 4	*Discuss policy and regulatory initiatives that advance infrastructure security and resilience priorities through robust coordination between government and industry.*
PRIORITY	1. Identify, prioritize, and support government research and development funding for critical financial infrastructure protection. 2. Identify and support policies that enhance critical financial infrastructure security and resilience, including a more secure and resilient Internet. 3. Encourage close coordination among firms, financial regulators, and executive branch agencies to inform policy development efforts.

Achieving Sector Goals

The Financial Services Sector enhances its security and resilience by leveraging the collective capabilities of a broad set of stakeholders. Much of this work is facilitated through the FSSCC and FBIIC via a series of collaborative working groups that target their efforts at achieving the sector's mission, vision, goals, and priorities as identified in the SSP.

The sector is already making progress toward achieving its goals around information sharing, best practices, incident response and recovery, and policy support. Ultimately, this ongoing work provides the foundation for the sector's approach to implementing the SSP.

Information Sharing

Sharing timely and actionable information is critical to managing cybersecurity and physical risk. To achieve this goal, public and private sector partners exchange data and contextual information about specific incidents and longer term trends and developments. Sharing this information helps to prevent incidents from occurring and reduces the risk of a successful incident at one firm impacting others. The Financial Services Sector's approach to sharing information involves integrating partners' security perspectives and insights to create shared awareness across the sector. These partners share information from government to the sector, from the sector to government, between institutions, across other sectors, and with international partners via an expanding and increasingly effective framework of information sharing mechanisms.

Much of the Financial Services Sector's technical information sharing is conducted by the FS-ISAC. Formed in 1999, the FS-ISAC is a member-owned non-profit and private Financial Services Sector initiative. It was designed and developed by its member institutions. Its primary function is to share timely, relevant, and actionable physical and cyber threat and incident information to enhance the ability of the Financial Services Sector to prepare for, respond to, and mitigate the risks associated with these threats. FS-ISAC gathers reliable and timely threat intelligence across the sector and from commercial security firms, government agencies, law enforcement, and other sectors. Through daily member-sharing and coordination with partners such as Treasury, the National Cybersecurity and Communications Integration Center (NCCIC), the Federal Bureau of Investigation, the National Council of ISACs, and other industry partners, FS-ISAC correlates and analyzes information and collaborates with partners to develop joint reports on threat intelligence, best practices, and mitigation strategies. With this broad situational awareness, FS-ISAC is able to identify physical and cybersecurity threat levels to keep the sector informed and prepared.

Financial Services Sector stakeholders also participate in information-sharing programs operated by government. For example, the FS-ISAC, some financial institutions, and Treasury maintain a presence within the NCCIC, which serves as a hub for sharing information related to cybersecurity and communications incidents across critical infrastructure sectors. This presence at the NCCIC includes strong participation in DHS' Cybersecurity Information Sharing and Collaboration Program (CISCP), which facilitates cybersecurity information sharing across sectors. The sector also works closely with the National Infrastructure Coordinating

Center (NICC), which is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of physical hazards impacting the nation's critical infrastructures for the Federal government. The Financial Services Sector also benefits greatly from its close information sharing relationship with law enforcement partners, including the Federal Bureau of Investigation and the United States Secret Service.

In addition, consistent with the directives of Presidential Policy Directive 21 and Executive Order 13636, Treasury operates the Financial Sector Cyber Intelligence Group (CIG) as part of the OCIP. The CIG identifies and analyzes all-source intelligence on cybersecurity threats to the Financial Services Sector; shares timely, actionable information that alerts the sector to threats and enables firms' prevention and mitigation efforts; and solicits feedback and information requirements from the sector. The CIG also works closely with the financial regulators through the FBIIC to share information.

Ensuring that information is delivered to those who need it quickly and in a form they can use is critical to any information sharing activity, especially cybersecurity information sharing where incidents can unfold instantaneously. In light of this, the sector, including many individual companies, the FS-ISAC, and Treasury, will continue to increase the speed and reliability of its information sharing efforts, including through expanded use of Structured Threat Information eXchange and Trusted Automated eXchange of Indicator Information which were developed as an open specification funded by DHS to enable the automated sharing of cybersecurity information.

Finally, it is critical to emphasize that in carrying out this information sharing partnership the Financial Services Sector and government are committed to ensuring that individual privacy and civil liberties protections are incorporated into all activities, to include technical analysis, information sharing on threats, and incident response efforts.

Best Practices

The Financial Services Sector works to raise the baseline protections of all firms. In light of the highly interconnected nature of the sector, a vulnerability at a vendor, customer, or counterparty has the potential to create a vulnerability for many other firms and possibly the entire sector. For this reason, financial institutions and government agencies work together to promote the use of common approaches and best practices for enhancing security and resilience to prevent incidents from occurring whenever possible.

Much of the sector's work in this area centers on assisting in the continued development and use of the NIST Cybersecurity Framework, both as a tool for individual firms to manage their internal risk and also as a tool for encouraging better security of vendors with whom the sector does business. The Framework, released in February 2014 following input from various Financial Services Sector and other stakeholders, provides companies with a flexible, repeatable, and cost-effective approach to manage cybersecurity-related risk. While the Framework is designed to manage cybersecurity risks, its core functions of Identify, Protect, Detect, Respond, and Recover provide a model for considering physical risks as well. This methodology is increasingly central to the sector's thinking on security and resilience, and the concept aligns with existing FFIEC guidance.

Financial Services Sector companies were closely involved in the development of the NIST Cybersecurity Framework, and continue to make progress in implementing it. This work has been aided not only by a close partnership with NIST, but also through the work of FSSCC, FBIIC, FS-ISAC, and sector trade associations, all of whom conduct workshops and promote the Framework's use at speaking engagements and conferences.

In addition, FSSCC and Treasury, along with DHS, are closely involved in efforts to promote the inclusion of the NIST Cybersecurity Framework into discussions about cybersecurity risk insurance which provides an important risk mitigation tool by allowing policyholders to transfer some financial exposure associated with cyber events.

In addition, the FFIEC issued a cybersecurity self-assessment tool in 2015 to help institutions identify their risks and determine their cybersecurity preparedness.

Incident Response and Recovery

Responding effectively to potential sector-wide incidents requires coordinated action among individual firms, security service providers, regulators, law enforcement, executive branch agencies, international partners, and others. To achieve this complex coordination, the sector maintains and continues to grow processes for facilitating whole-of-sector response to incidents and for coordinating these response efforts with government partners. These processes are consistent with the framework established by Presidential Policy Directive 8 and the National Response Framework and include, for example:

- Mechanisms for quickly sharing information about identified incidents to alert others and mitigate further impacts;
- Established processes for institutions to request technical cybersecurity assistance from government; and
- Procedures for coordinating with international partners and the media.

Importantly, the sector's response and recovery processes are regularly exercised not only to test and enhance plans, but also to sustain strong organizational relationships between incident responders. Such exercise efforts directly inform and help to improve the sector's ability to respond individually and collaboratively to various attack scenarios.

Policy Support

Facilitation of the sector's security and resilience work requires an effective public policy framework that is appropriately informed by private sector perspectives. Public-private partnerships enable government and private sector partners to discuss how public policy proposals and implementation can evolve to support the protection of the Nation's critical financial infrastructure most effectively.

For example, government agencies provide significant resources to develop new technologies to

support critical infrastructure security and resilience. These resources can be most effectively leveraged when their development is informed by the perspectives of the private sector owners and operators of critical infrastructure. Accordingly, the FSSCC has developed research and development (R&D) priorities to help inform R&D resource allocation decision-making by government agencies, such as the DHS Office of Science and Technology Policy and the National Science Foundation.

Collaborative efforts to inform public policy processes appropriately provide a means for addressing dynamic risk through voluntary engagement and collaboration in addition to regulation. For the financial regulators, voluntary programs provide insights into sector-wide resilience efforts and allow for important information-sharing and risk management procedures, in addition to traditional regulatory discussions and processes.

Measuring Effectiveness

Working groups established among the FSSCC and FBIIC, with frequent participation from other partners, meet regularly to plan and execute security and resilience projects based on the priorities defined in this SSP. In order to measure progress and assess the effectiveness of these efforts, working groups develop specific action plans and identify key milestones and expected outcomes for advancing and ultimately accomplishing each priority.

To help ensure accountability, the FBIIC and the FSSCC meet jointly to discuss progress toward achieving the sector's goals and priorities and to identify areas where additional work is needed. The FBIIC and FSSCC meet separately at least once a month to provide status reports on projects and initiatives and to coordinate new and existing programs. This engagement allows the FSSCC and FBIIC to track progress based on an evolving set of project milestones. This approach has resulted in, for example, developing and executing an ongoing public-private cybersecurity exercise program, coordinating regular analytical discussions of cybersecurity threats between government and the private sector, and the refinement of incident response processes.

In addition, continuously assessing the sector's progress, developing new programs as needed, and standing down programs that have served their purpose helps to ensure that individual activities are responsive to stakeholder needs and can be effectively tailored to the evolving threat environment.

Appendix A: Contribution of Sector Priorities to the Joint National Priorities and NIPP Goals

FINANCIAL SERVICES SECTOR GOALS	Joint National Priorities (DRAFT)					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	
1. Implement and maintain structured routines for sharing timely and actionable information related to cybersecurity and physical threats and vulnerabilities among firms, across sectors of industry, and between the private sector and government.	*Goal 1*		*Goal 1*	*Goal 1*	*Goal 1*	Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
2. Improve risk management capabilities and the security posture of firms across the Financial Services Sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.	*Goal 2*		*Goal 2*			Assess and analyze risks to critical infrastructure (based on the NIPP Risk Management concept of threat, vulnerabilities, and consequences to inform risk management activities.
				Goal 2		Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.

FINANCIAL SERVICES SECTOR GOALS	Joint National Priorities (DRAFT)					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	
3. Collaborate with the homeland security, law enforcement, and intelligence communities; financial regulatory authorities; other sectors of industry; and international partners to respond to and recover from significant incidents.		*Goal 3*	*Goal 3*			Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery.
		Goal 3	*Goal 3*		*Goal 3*	Promote learning and adaptation during and after incidents and exercises.
4. Discuss policy and regulatory initiatives that advance infrastructure security and resilience priorities through robust coordination between government and industry	*Goal 4*	*Goal 4*	*Goal 4*	*Goal 4*		Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.
	Goal 4	*Goal 4*	*Goal 4*	*Goal 4*		Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery.

This page intentionally left blank.