THE WHITE HOUSE
WASHINGTON

April 30, 2024

NATIONAL SECURITY MEMORANDUM/nSM-22

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF THE INTERIOR
THE SECRETARY OF AGRICULTURE
THE SECRETARY OF COMMERCE
THE SECRETARY OF HEALTH AND HUMAN SERVICES
THE SECRETARY OF HOUSING AND URBAN DEVELOPMENT
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE SECRETARY OF EDUCATION
THE SECRETARY OF HOMELAND SECURITY
THE ASSISTANT TO THE PRESIDENT AND CHIEF OF STAFF
THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS

THE ASSISTANT TO THE PRESIDENT AND HOMELAND SECURITY ADVISOR
THE ASSISTANT TO THE PRESIDENT AND DIRECTOR OF THE NATIONAL ECONOMIC COUNCIL
THE ASSISTANT TO THE PRESIDENT AND DIRECTOR OF THE OFFICE OF INTERGOVERNMENTAL AFFAIRS
THE ADMINISTRATOR OF THE ENVIRONMENTAL PROTECTION AGENCY
THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF NATIONAL INTELLIGENCE
THE DIRECTOR OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF
THE ADMINISTRATOR OF GENERAL SERVICES
THE CHAIR OF THE NUCLEAR REGULATORY COMMISSION
THE CHAIR OF THE FEDERAL COMMUNICATIONS COMMISSION
THE NATIONAL CYBER DIRECTOR
THE POSTMASTER GENERAL AND CHIEF EXECUTIVE OFFICER OF THE UNITED STATES POSTAL SERVICE

SUBJECT: Critical Infrastructure Security and Resilience

Critical infrastructure comprises the physical and virtual assets and systems so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety. It is diverse and complex, and includes distributed networks,

varied organizational structures, operating models, interdependent systems, and governance constructs.

The United States is in the midst of a generational investment in the Nation's infrastructure. This investment, and the emergence of new technologies, presents an opportunity to build for the future. In the 21st century, the United States will rely on new sources of energy, modes of transportation, and an increasingly interconnected and interdependent economy. This modernization effort will ensure critical infrastructure provides a strong and innovative economy, protects American families, and enhances our collective resilience to disasters before they happen -- creating a resilient Nation for generations to come.

The United States also faces an era of strategic competition with nation-state actors who target American critical infrastructure and tolerate or enable malicious actions conducted by non-state actors. Adversaries target our critical infrastructure using licit and illicit means. In the event of crisis or conflict, the Nation's adversaries will also likely increase their efforts to compromise critical infrastructure to undermine the will of the American public and jeopardize the projection of United States military power. The growing impact of climate change, including changes to the frequency and intensity of natural hazards, as well as scarcities; supply chain shocks; and the potential for instability, conflict, or mass displacement places further strain on the assets and systems that Americans depend upon to live and do business.

This memorandum advances our national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Policy Principles and Objectives

It is the policy of the United States to strengthen the security and resilience of its critical infrastructure, consistent with the following principles:

1. Shared Responsibility. Safeguarding critical infrastructure is a responsibility shared by Federal, State, local, Tribal, and territorial entities, and the public or private owners and operators of critical infrastructure (owners and operators). All stakeholders have unique roles to contribute to the national unity of effort. Public-private collaboration is vital to this effort.

2. Risk-Based Approach. Advancing critical infrastructure security and resilience requires a risk-based approach. The prioritization of national efforts must be informed by the relationship between specific infrastructure and national security (including national defense), national economic security, national public health or safety, and the Federal Government's ability to perform essential functions and services. Risk assessments must consider all threats and hazards, likelihood, vulnerabilities, and consequences, including shocks and stressors -- as well as the scope and scale of dependencies within and across critical infrastructure sectors, immediate and long-term consequences, and cascading effects. Owners and operators are uniquely positioned to manage risks to their individual operations and assets, including their interdependencies with other entities and sectors.

3. Minimum Requirements. Federal, State, local, Tribal, and territorial regulatory and oversight entities have a responsibility to prioritize establishing and implementing minimum requirements for risk management, including those requirements that address sector-specific and cross-sector risks. These requirements should also leverage existing guidance where applicable. Regulatory frameworks should be risk- and performance-based when feasible; informed by existing requirements, standards, and guidelines; aligned to reduce unnecessary duplication; complementary to voluntary public-private collaboration; and scalable and adaptable to an evolving risk environment. Requiring and enforcing minimum resilience and security requirements and recommendations that direct building resilience into critical infrastructure assets and systems upfront, and by-design, shall be a primary responsibility of the Federal Government.

4. Accountability. Robust accountability and enforcement mechanisms from Federal, State, local, Tribal, territorial, and private sector entities, as well as independent third parties, are an essential component of effective risk management for critical infrastructure. Accountability mechanisms should continuously evolve to keep pace with the Nation's risk environment.

5. Information Exchange. The appropriate sharing of timely, actionable information, which may include relevant classified and unclassified intelligence and law enforcement sensitive

information, among Federal, State, local, Tribal, and territorial entities; owners and operators; and other relevant stakeholders, is essential for effective risk management. The Federal Government will support a robust information sharing environment and public-private cooperation that enables actions and outcomes that reduce risk.

6. Expertise and Technical Resources. The Federal Government will leverage expertise and technical resources from all relevant Federal departments and agencies to mature the capacity and capability of each federally led effort to manage sector-specific risk under the umbrella of the national effort to secure United States critical infrastructure. A primary objective of this effort will be to create a consistent experience for owners and operators; State, local, Tribal, and territorial governments; and other essential stakeholders who collaborate with the Federal Government.

7. International Engagement. Recognizing the global interconnectedness and interdependencies of critical infrastructure, the Federal Government will work closely with international partners to strengthen the security and resilience of the international critical infrastructure on which the United States depends.

8. Policy Alignment. Efforts to safeguard critical

infrastructure will be fully integrated and coordinated with complementary Federal policies and frameworks, including domestic incident management and national preparedness; national continuity, including Federal Mission Resilience; and counterterrorism, counterintelligence, cybersecurity, and other threat-, hazard-, or sector-specific policies and frameworks.

It is the objective of the United States under this national effort to:

1. Refine and clarify the roles and responsibilities of the Federal Government for critical infrastructure security, resilience, and risk management.

2. Identify and prioritize critical infrastructure security and resilience based on risk and implement a coordinated national approach to assess and manage sector-specific and cross-sector risk.

3. Establish minimum requirements and accountability mechanisms for the security and resilience of critical infrastructure, including through aligned and effective regulatory frameworks.

4. Leverage Federal Government agreements, including grants,

loans, and procurement processes, to require or encourage owners and operators to meet or exceed minimum security and resilience requirements.

5. Enhance and improve the quality of intelligence collection and analysis pertaining to threats to critical infrastructure.

6. Improve the real-time sharing of timely, actionable intelligence and information at the lowest possible classification level among Federal, State, local, Tribal, territorial, private sector, and international partners to facilitate risk mitigation to critical infrastructure.

7. Promote timely and cost-effective investments in technologies and solutions that mitigate risk from evolving threats and hazards to critical infrastructure.

8. Strengthen the security and resilience of critical infrastructure by engaging international partners and allies to build situational awareness and capacity, facilitate operational collaboration, promote effective infrastructure risk management globally, and develop and promote international security and resilience recommendations.

Federal departments and agencies shall implement this memorandum in a manner consistent with applicable law; Presidential directives; and Federal regulations, including those protecting privacy, civil rights, and civil liberties.

Roles and Responsibilities

The Federal Government relies on the specialized authorities, capabilities, and expertise of Federal departments and agencies to ensure an effective, whole-of-government effort to secure critical infrastructure. Under this effort, the Secretary of Homeland Security shall provide strategic guidance and coordinate Federal cross-sector risk management and resilience activities. Sector Risk Management Agencies (SRMAs) shall serve as day-to-day Federal interfaces for their designated critical infrastructure sector and conduct sector-specific risk management and resilience activities. Elements of the Intelligence Community (IC) and law enforcement, regulatory, and other Federal departments and agencies also play key roles in increasing the security and resilience of critical infrastructure, including responding to all threats and hazards that may affect critical infrastructure.

Close and continuous coordination among the Department of Homeland Security (DHS), SRMAs, and other relevant Federal departments and agencies, to include law enforcement and the IC, is essential to ensuring a national unity of effort and accomplishing the objectives of this memorandum. The Federal Government also seeks to encourage and enable strong collaboration with owners and operators; State, local, Tribal, and territorial governments; international partners; and other entities. While most of the Nation's critical infrastructure is owned and operated by non-Federal entities, which are primarily responsible for individual assets' security and resilience, both Government and the private

sector have a mutual responsibility and incentive to reduce the risk to critical infrastructure.

Secretary of Homeland Security

The Secretary of Homeland Security shall coordinate the national effort to enhance the security and resilience of United States critical infrastructure and provide strategic guidance on this national effort, based on national priorities and sector-specific or cross-sector risk assessments and plans, including through the National Infrastructure Risk Management Plan (National Plan), as required by statute. The Secretary of Homeland Security shall maintain situational awareness about emerging trends, imminent threats, vulnerabilities, and the consequences of incidents that could jeopardize the security and resilience of critical infrastructure. The Secretary of Homeland Security shall make recommendations to the President, in coordination with SRMAs and other relevant departments and agencies, on the list of designated critical infrastructure sectors, subsectors, and SRMAs -- prioritizing critical infrastructure for national security and resilience efforts.

The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA) as the National Coordinator for the Security and Resilience of Critical Infrastructure (National Coordinator), shall, in coordination with SRMAs and other Federal departments and agencies:

1. Coordinate with SRMAs to fulfill their roles and responsibilities to implement national priorities consistent with strategic guidance and the National Plan and continuously strengthen a unified approach to critical

infrastructure security and resilience;

2. Assess progress against national priorities and national resilience and support efforts that measure and enhance the strength of critical infrastructure sectors and partnerships;

3. Identify and assess sector and cross-sector risk, analyze the dependencies among assets and systems that comprise critical infrastructure, and consider key interdependencies of potential sector and cross-sector consequences associated with physical and cyber threats and vulnerabilities to support critical infrastructure risk management and prioritization;

4. Assess sector and SRMA designations to inform recommendations to the President;

5. Recommend measures to protect the critical infrastructure of the United States; and

6. Identify security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors.

To provide expertise in support of national critical

infrastructure security and resilience efforts, the Director of CISA, in coordination with SRMAs and, as appropriate, other relevant agencies, shall also:

1. Provide capabilities and resources, such as cybersecurity expertise, risk assessments, and other services, to support SRMAs and national critical infrastructure security and resilience efforts;

2. Develop plans and enable integrated actions for cyber defense campaigns at scale and to otherwise mitigate risks to critical infrastructure nationally;

3. Engage international partners to enhance the security and resilience of critical infrastructure globally; and

4. Provide technical and operational assistance, best practices based on existing standards and guidance to the greatest extent possible, and capacity development to State, local, Tribal, and territorial governments; other Federal entities; owners and operators; and international partners to enhance the security and resilience of critical infrastructure.

Other Department of Homeland Security Activities

As reflected in statute and Presidential policy, the Secretary of

Homeland Security has responsibilities for coordinating Federal preparedness activities and response operations in the United States, including when critical infrastructure impacts are implicated. The Secretary of Homeland Security is the principal Federal official for domestic incident management and, consistent with existing Federal law and policy, including Homeland Security Presidential Directive 5 of February 28, 2003 (Management of Domestic Incidents), as amended, DHS may coordinate Federal Government resources used in the response to or recovery from terrorist attacks, major disasters, or other emergencies, or as otherwise requested or directed by the President. In addition, the Secretary of Homeland Security, acting through the Administrator of the Federal Emergency Management Agency (FEMA), works to reduce the loss of life and property by minimizing the impact of disasters and protecting the Nation from all hazards. DHS, acting through the Director of CISA, serves as the lead Federal agency for cyber asset response activities in accordance with Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination) (PPD-41). Further, the Secretary of Homeland Security, acting through the Administrator of the Transportation Security Administration and the Commandant of the United States Coast Guard, has broad authority to assess security risks to the Marine Transportation System and other modes of transportation, develop security measures and regulations, and seek or ensure compliance with those measures and regulations.

Sector Risk Management Agencies

Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified SRMA with institutional knowledge, specialized expertise, and established relationships across the sector. SRMAs help drive the national effort to strengthen the security and resilience of

critical infrastructure. Consistent with the statutorily defined roles and responsibilities of SRMAs, SRMAs shall carry out the following roles and responsibilities for their respective sectors, in coordination with DHS, including the National Coordinator, and, as appropriate, other relevant departments and agencies:

1. Serve as day-to-day Federal interfaces for the prioritization and coordination of sector-specific activities, including the provision of technical expertise and assistance, serving as the Federal Government coordinating council chair; and participating in cross-sector coordinating councils. Continually collaborate and communicate through regular and appropriate outreach and engagement mechanisms with their sector's owners and operators, promoting the use of risk mitigation, to include Government-furnished capabilities and services for State, local, Tribal, and territorial governments; owners and operators; and other non-Federal entities.

2. Lead outreach to owners and operators within their respective sectors on security and resilience issues, consistent with their available authorities.

3. Designate the Accountable Senior Officials -- Assistant Secretary equivalent or above -- to serve as the Coordinators of the SRMA Function, with the ability to delegate responsibilities to other senior leaders within their agencies. The designees will be responsible and accountable for the implementation and performance of all SRMA roles and

responsibilities.

4. Lead sector risk management within their sector and support cross-sector risk management, including establishing and implementing programs or initiatives to assist owners and operators and State, local, Tribal, and territorial governments with identifying, understanding, planning for, and mitigating risks to the systems, assets, or services in their respective sector. This should include recommending sector-specific measures to protect critical infrastructure.

5. Identify, assess, and prioritize sector-specific risk and support cross-sector and national risk assessment efforts.

6. Facilitate the identification of essential critical infrastructure-related workforce needs and priorities for security and resilience.

7. Incorporate identified national priorities, including Defense Critical Infrastructure (DCI), climate change, and emerging technology, into sector risk management responsibilities.

8. Identify sector-specific information and intelligence needs and priorities, in consultation with owners and operators, and facilitate the exchange of information and intelligence,

as appropriate, regarding risks to sector-specific critical infrastructure.

9. Share and receive information and intelligence directly with critical infrastructure owners and operators in their respective sectors, as appropriate and in coordination with the IC.

10. Support domestic incident management, emergency preparedness, and national continuity, including Federal Mission Resilience.

11. Serve as the lead Federal agencies for certain domestic incidents primarily impacting their respective sectors consistent with existing Federal law and policy, including when requested or directed by the President.

12. Provide, support, or facilitate the provision of technical assistance to sectors' owners and operators to mitigate risk, and collaborate with those owners and operators to identify joint priorities that enhance the security and resilience of the sectors.

Additional Federal Roles and Responsibilities

1. The Federal Senior Leadership Council (FSLC) shall be the consensus-based body that coordinates and deconflicts the shared responsibilities and activities of Federal departments and agencies under this policy, and will be informed by engagement with the National Security Council. The FSLC shall be co-chaired by the Director of CISA and a non-CISA Accountable Senior Official for an SRMA that serves a 2-year term. The co-chairs shall coordinate regularly with each SRMA's respective Accountable Senior Official on all sector-specific activity and regularly brief the FSLC on cross-sector initiatives, including the sharing of best practices, data, and tools from those initiatives. The FSLC shall, at least annually, communicate to SRMAs national and cross-sector guidance and priorities for SRMA efforts. SRMAs shall provide regular updates to the FSLC on the implementation of their roles and responsibilities and on the implementation of FSLC guidance and priorities. The FSLC shall develop shared SRMA processes and doctrine. If there is a conflict between members that cannot be resolved through consensus at the FSLC, it will be elevated to the National Security Council for resolution.

2. The Department of State shall lead the effort to engage foreign governments, international organizations, and international partners -- in coordination with other Federal departments and agencies -- to facilitate collaboration and capacity building and to strengthen the security and resilience of foreign critical infrastructure upon which the Nation depends.

3. The Department of Defense (DOD) shall lead the evaluation of the risk to and prioritization of mitigations for sector-specific DCI, in coordination with the National Coordinator, the IC, and relevant SRMAs. DOD shall provide DHS, relevant SRMAs, and other Federal departments and agencies with advice to further these efforts and support sector and cross-sector outreach to strengthen the security and resilience of non-DOD-owned DCI. As part of its national defense mission, DOD supports defense of critical infrastructure.

4. The Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), shall lead counterterrorism and counterintelligence law enforcement activities for critical infrastructure. Such activities include leading criminal investigations into and the operational response to terrorist threats and incidents that concern critical infrastructure -- including those that involve weapons of mass destruction, sabotage, and counterintelligence threats -- and the identification of critical infrastructure owner and operator information requirements to inform collection and analysis. The FBI shall, as appropriate, coordinate with DHS, SRMAs, and other law enforcement entities or Federal departments and agencies. In the event of significant cyber incidents involving critical infrastructure, DOJ, acting through the FBI and the National Cyber Investigative Joint Task Force, shall carry out its responsibilities as the Federal lead agency coordinating for threat response activities under PPD-41.

5. The Department of Commerce shall carry out its statutory responsibilities to lead the development of standards and to facilitate and support guidelines, best practices, methodologies, procedures, and processes to reduce cybersecurity risks to critical infrastructure. The Department of Commerce shall consult with DHS and engage with other Federal departments and agencies, as well as with the private sector, research organizations, academic organizations, or other Government organizations, to: (1) improve security for hardware and software technologies and associated tools related to cyber-based systems; (2) improve resilience standards, guidelines, best practices, tools, technologies, testing, and references for physical infrastructure and social or economic systems; and (3) promote the development of other efforts related to critical infrastructure to enable the timely availability of industrial products, materials, and services to meet homeland security requirements.

6. The Department of Energy (DOE) shall carry out its statutory responsibilities to address the short-, mid-, and long-term energy challenges facing the Nation, including those implicating electricity, petroleum, natural gas, nuclear material, and other energy resources and services, in coordination with relevant Federal departments and agencies, as appropriate. Consistent with authorities, DOE leads the policy, preparedness, risk analysis, technical assistance, research and development, operational collaboration, and emergency response activities for the United States energy

sector.

7. The IC, led by the Director of National Intelligence (DNI), shall coordinate with DHS and SRMAs to identify critical infrastructure owner and operator intelligence needs. The IC shall provide intelligence to the National Coordinator and SRMAs regarding threats to critical infrastructure and coordinate on intelligence and other sensitive or proprietary information related to critical infrastructure, as appropriate. In the event of significant cyber incidents involving critical infrastructure, the DNI, acting through the Director of the Cyber Threat Intelligence Integration Center, shall carry out its responsibilities as the Federal lead agency for intelligence support and related activities under PPD-41.

8. The Director of the National Security Agency, as the National Manager for National Security Systems (NSS), shall assess the overall security posture of NSS, disseminate information on threats to and vulnerabilities of NSS, and direct actions for cybersecurity-related improvements needed on NSS. NSS that are owned, operated, managed, or used by a Federal entity are not otherwise subject to the requirements of this memorandum. In addition, information security policies, directives, standards, and guidelines for safeguarding NSS shall be overseen as directed by the President or applicable law, and in accordance with that direction, shall be carried out under the authority of the heads of agencies that operate or exercise authority over such NSS.

9. The General Services Administration (GSA), in consultation with DOD, DHS, and other departments and agencies, shall provide or support Government-wide contracts for critical infrastructure assets and systems, and shall ensure that such contracts include appropriate audit rights for the security and resilience of critical infrastructure, including the cybersecurity of critical infrastructure-enabling technology.

10. The Nuclear Regulatory Commission (NRC) shall oversee its licensees' protection of commercial nuclear power reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings, and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste. As appropriate, the NRC shall collaborate with DHS, DOJ, DOE, the FBI, FEMA, and other Federal departments and agencies on strengthening critical infrastructure security and resilience.

11. The Federal Communications Commission will, to the extent permitted by law and in coordination with DHS and other Federal departments and agencies: (1) identify and prioritize communications infrastructure by collecting information regarding communications networks; (2) assess communications sector risks and work to mitigate those risks by requiring, as appropriate, regulated entities to take specific actions to protect communications networks and infrastructure; and (3) collaborate with communications

sector industry members, foreign governments, international organizations, and other stakeholders to identify best practices and impose corresponding regulations.

12. In accordance with applicable law and policy, Federal departments and agencies shall exchange timely data and information with DHS necessary to assess and manage risks to critical infrastructure, and with the FBI to assist in relevant law enforcement activities.

13. In accordance with applicable law and policy, Federal departments and agencies with regulatory authorities shall utilize regulation, drawing on existing voluntary consensus standards as appropriate, to establish minimum requirements and effective accountability mechanisms for the security and resilience of critical infrastructure. Departments and agencies shall work to harmonize these efforts to the maximum extent possible through participation in Federal interagency working groups, such as the Cybersecurity Forum for Independent and Executive Branch Regulators. Departments and agencies shall continue to support the development of voluntary consensus standards that enable critical infrastructure innovation to occur in a secure and resilient manner that considers the impacts and effects of risk.

14. Federal department and agency heads are responsible for activities concerning the identification, prioritization, assessment, remediation, and security of their respective

internal critical infrastructure and associated infrastructure that supports mission essential functions. Infrastructure supporting primary mission essential functions shall be addressed in the plans and execution of the requirements in all applicable Executive Orders, National Continuity Policies, strategies, and directives.

15. Consistent with applicable law and policy, Federal departments and agencies, regardless of designation as an SRMA, shall leverage existing authorities to promote security and resilience of critical infrastructure including, but not limited to:

a. Integrating security and resilience into Federal acquisition programs relating to critical infrastructure.

b. Utilizing grants, loans, and other Federal Government funding mechanisms to ensure minimum security and resilience requirements and effective accountability mechanisms are incorporated into critical infrastructure-related projects that receive Federal funding, where determined necessary to mitigate risk by the administering departments or agencies. Where applicable law limits the ability of Federal departments and agencies to establish minimum requirements through agreements, they shall provide guidance and recommendations for appropriate security and resilience measures alongside the provision of Federal funding.

16. Interagency bodies, such as the Committee on Foreign Investment in the United States and the Federal Acquisition Security Council, have specific roles in protecting and securing critical infrastructure through the review of foreign investment transactions, and shall leverage existing authorities to also address the risks to critical infrastructure posed by foreign investment activity, and supply chain reliability and illicit access to sensitive information, respectively.

Risk Management

The Federal Government, including SRMAs, shall use a common risk-based approach to reducing risk to critical infrastructure. Critical infrastructure risks can be assessed in terms of threats or hazards, vulnerability, and consequence. For the purposes of this effort, the term "risk" refers to the potential for an unwanted outcome, as determined by its likelihood and the consequences. Risk management efforts should be prioritized based on this shared definition, which necessitates identifying the criticality of assets and systems within and across sectors.

Asset-level Risk

Critical infrastructure owners and operators have primary responsibility, and are uniquely positioned, to manage most risks to their operations and assets. The policy of the Federal Government shall be to support and guide the entities that own, operate, or otherwise control critical infrastructure assets and systems by providing these entities with the information,

intelligence analysis, and other support, as appropriate, to manage and mitigate asset-level risks.

Nationally Significant Risk

Effective risk management necessitates the Federal Government, in coordination with owners and operators to the extent practicable, identify, assess, prioritize, mitigate, and monitor risks that may have a potentially debilitating impact on national security (including national defense and continuity of Government), national economic security, or public health or safety. These nationally significant risks may arise within and impact particular sectors or cut across multiple sectors. Federal departments and agencies have the responsibility to identify and mitigate national-level risk through this whole-of-government effort based on the roles and responsibilities enumerated in statute, regulation, and this memorandum. This effort shall be led by DHS in coordination with SRMAs and supported by other Federal departments and agencies with the necessary expertise, resources, and regulatory authorities to support or direct risk mitigation activity. Federal departments and agencies shall leverage all available resources, capabilities, and authorities -- including regulatory authorities -- to ensure owners and operators implement risk mitigation measures that limit national-level risks. This work shall be coordinated by the National Coordinator, in consultation with the National Security Council staff and the National Cyber Director, as appropriate.

Sector Risk

Certain risks that rise to national concern are common to entities within a particular sector. SRMAs are responsible for day-to-day prioritization and coordination of efforts to mitigate risks within each sector, as part of the broader whole-of-government effort

coordinated by DHS, including the National Coordinator, to secure United States critical infrastructure. The Federal Government will support owners and operators as they manage sector-level risk to individual assets and systems.

Systemic and Cross-sector Risk

Critical infrastructure has grown increasingly interdependent and interconnected due to trends in the modern economy, including digitization and electrification. These trends are poised to accelerate over the coming decade due to historic Federal investments in the modernization of the Nation's infrastructure. As such, risks to individual sectors can quickly cascade into other sectors, necessitating coordinated action to understand and mitigate risk.

The National Coordinator shall actively manage systemic and cross-sector risk by working with SRMAs, Federal departments and agencies, and industry to identify, analyze, prioritize, and manage the most significant risks involving multiple sectors. To identify and manage cross-sector risk, SRMAs shall regularly provide the National Coordinator available data on individual assets and systems within their respective sectors. The National Coordinator shall aggregate and analyze this data to improve the identification, prioritization, and mitigation of cross-sector and national risks, and shall provide this analysis to SRMAs to help manage sector-specific risk.

Minimum Security and Resilience Requirements

Effective risk management will require consistent adoption of minimum security and resilience requirements, where possible based on established consensus-based standards, within and across

critical infrastructure sectors. Voluntary approaches to enhance critical infrastructure security and resilience have meaningfully mitigated risk over the past decade, but more must be done to ensure the Nation's critical infrastructure is secure and resilient against all threats and hazards. The Federal Government must focus on increasing the adoption of requirements that address sector, national, and cross-sector risks to critical infrastructure.

DHS, including the National Coordinator, SRMAs, and, as appropriate, regulators, shall coordinate to produce cross-sector and sector-specific guidance, performance goals and metrics, and requirements, consistent with their authorities, to adequately mitigate risk. SRMAs, in coordination with regulators, as appropriate and consistent with their authorities, shall develop sector-specific minimum security and resilience requirements for each respective sector, as necessary, and a plan to use existing authorities or other tools to effectively implement those requirements. SRMAs shall support the development of sector-specific performance goals in accordance with National Security Memorandum 5 of July 28, 2021 (Improving Cybersecurity for Critical Infrastructure Control Systems).

The National Coordinator shall review proposed sector-specific security and resilience guidance, performance goals, and requirements in coordination with SRMAs, and in consultation with regulators, to facilitate the harmonization of these directives and recommendations at the national and cross-sector level. The National Coordinator shall also provide input into the development of these requirements and recommendations to ensure they address cross-sector and national-level risk, while integrating voluntary standards and mandatory requirements into overall risk management plans and helping to prevent the promulgation of conflicting directives or requirements across sectors. In accordance with the

National Cybersecurity Strategy, the National Cyber Director, in coordination with the Director of the Office of Management and Budget, shall lead my Administration's efforts for cybersecurity regulatory harmonization with respect to security and resilience requirements, of which portions of the effort outlined in this memorandum are an essential component.

Operational Collaboration

To further drive down the Nation's risk, the Federal Government must improve its ability to collaborate directly with those partners who have the means and capability to take actions that mitigate vulnerabilities, respond to incidents, and build resilience at scale. This will complement individual owners and operators' risk mitigation efforts. The Federal Government will collaborate with private-sector partners; State, local, Tribal, and territorial governments; community organizations; and international partners who can take actions that provide resilience and security benefits to owners and operators in the United States and in other countries.

National Infrastructure Risk Management Plan

The Secretary of Homeland Security shall develop and submit to the President on a recurring basis every 2 years a National Infrastructure Risk Management Plan (National Plan), which shall be informed by: (1) individual sector-specific risk assessments and risk management plans; and (2) a cross-sector risk assessment.

Sector-specific Components

Each SRMA shall develop sector-specific risk assessments and sector-specific risk management plans based on strategic direction

provided by the Secretary of Homeland Security, or as prescribed in another National Security Memorandum.

- Sector-specific Risk Assessment: Unless otherwise defined in another National Security Memorandum, each SRMA shall, on a biennial basis, and in consultation with their sector coordinating councils, identify the most significant critical infrastructure risks to their sector, including key cross-sector risks and interdependencies. This review shall be based on appropriate Federal, State, local, Tribal, and territorial government-level data and analysis, enforcement actions, and guidance, as well as information from relevant private sector partners, regulators, intelligence analysts, and law enforcement professionals. The risk assessment shall use all available information and intelligence to identify the risks presented by the current threat environment to critical infrastructure within the covered sector.

- Sector-specific Risk Management Plan: Each SRMA shall, on a biennial basis, develop or refresh, in consultation with their sector coordinating councils, a sector-specific risk management plan to leverage both individual SRMA tools and authorities, as well as other Federal tools and authorities, to safeguard critical infrastructure in their sector from all threats and hazards. The plan will take into account national-level priorities and guidance from the Secretary of Homeland Security, as well as other changes in the critical infrastructure risk environment and any deficiencies in the sector's current risk management approach. The sector-specific plan shall also prioritize specific risks and

establish corresponding lines of effort that affect resourcing decisions to mitigate risk to critical infrastructure. The plan is intended to prioritize threats based on the sector-specific risk assessment. These efforts shall include:

- A proposal for any necessary authorities to ensure the Federal Government can incentivize and compel the owners and operators to adequately address sector-level risk from all threats and hazards, including:

- The identification, harmonization, or development of recommended, sector-specific minimum security and resilience requirements, consistent with their authorities, for each respective sector based on national and cross-sector security and resilience requirements -- and a plan to use existing tools and authorities to implement those requirements across the sector. SRMAs shall coordinate with relevant regulators on the adoption of regulations that promote the implementation of these minimum requirements concurrently with the submission of the National Plan to the President. Where existing authorities are not sufficient, SRMAs shall develop a proposal to request new authorities from the Congress, in coordination with the Office of Management and Budget, the National Security Council, and, to the extent such authorities pertain to cybersecurity, the Office of the National Cyber Director.

- Prioritized lines of effort the SRMA plans to undertake over the next 2 years to mitigate risk to critical infrastructure in their sector, including: efforts to collaborate with law enforcement; State, local, Tribal, and territorial governments; and other domestic or international partners.

- A plan to leverage technological innovation to stay ahead of evolving trends, including coordination on research and development with relevant Federal laboratories.

- A description of each respective sector's information sharing strategy.

- A set of objective measures of success that track the overall security and resilience of the sector and critical assets or systems within the sector.

- For the second biennial National Plan and each one thereafter, an assessment of progress made over the prior 2 years in implementing the previous sector-specific risk management plan.

Sector risk assessments previously directed by statute or executive action will be integrated with the sector-specific risk assessments

outlined in this memorandum whenever practical. This integration improves cross-sector security and resilience planning. The National Coordinator and SRMAs will coordinate to synchronize the reporting cycle of risk reporting to improve efficiency and reduce duplication of effort. Government-specific portions of the sector-specific risk assessments should also be shared with the GSA.

Cross-sector Risk Assessment

The National Coordinator shall develop a cross-sector risk assessment in coordination with SRMAs, and share this assessment with SRMAs.

- The cross-sector risk assessment shall identify the most significant cross-sector risks to United States critical infrastructure. This review shall be based on Federal and State-level data and analysis, enforcement actions, and guidance, as well as interviews with relevant private sector partners, SRMA staff, regulators, intelligence analysts, and law enforcement professionals. The cross-sector risk assessment shall use all available information and intelligence to identify the risks presented by the current threat environment to critical infrastructure, with a focus on cross-sector risk. This cross-sector risk assessment will identify risks that span across sectors, including where multiple sectors depend on the same materials or technologies, as well as risks with consequences that cascade across sectors that may be difficult to identify or assess without the cross-sector understanding.

National Infrastructure Risk Management Plan

Based on the sector-specific risk assessments and risk management plans and the cross-sector risk assessment, the Secretary of Homeland Security shall develop and submit to the President, through the Assistant to the President and Homeland Security Advisor, the National Plan to guide the Federal effort to mitigate cross-sector and other national risks to critical infrastructure.

This forward-looking National Plan shall identify avenues to leverage all available Federal tools, resources, and authorities to limit national-level risks, including those cascading across sectors of critical infrastructure. The National Plan shall also prioritize specific cross-sector risks, with a focus on new and emerging threats to critical infrastructure, and shall identify innovative approaches to limit the risks from these new and emerging threats, particularly risk mitigation strategies for increasingly interdependent and interconnected assets and systems. This document shall be the Federal Government's comprehensive plan to mitigate and manage cross-sector risk -- identifying and funding sensible mitigation actions and investments across sectors, as well as continuously identifying for interagency policymakers the gaps and limitations in existing Federal tools or authorities to address the rapidly changing threat and hazard landscape. The National Plan shall also contain:

- Proposed long-term mitigation activities based on sector-specific and cross-sector risk assessments to incorporate resilience-by-design approaches that enhance the ability of critical infrastructure to prepare for, adapt to, and recover from changing conditions presented by new and emerging threats and hazards.

- The identification, harmonization, and development of recommended national and cross-sector minimum security and resilience requirements to mitigate cross-sector risks not covered under sector-specific requirements, and a plan to use existing tools and authorities to implement those requirements. Where existing authorities are not sufficient to implement these minimum requirements, the National Coordinator shall develop a proposal to request new authorities from the Congress, in coordination with other relevant Federal departments and agencies, the Office of Management and Budget, the National Security Council, and, to the extent such authorities pertain to cybersecurity, the Office of the National Cyber Director.

- A plan for harmonizing minimum security and resilience requirements across all sectors based on input from SRMAs and other relevant Federal departments and agencies. The National Coordinator, in coordination with regulators, SRMAs, and other appropriate Federal departments and agencies, shall lead this all-hazards effort. The National Cyber Director, in coordination with the Director of the Office of Management and Budget, shall continue to lead my Administration's efforts for cybersecurity regulatory harmonization.

- Recommendations for pilot efforts, led by SRMAs or the National Coordinator, to limit the risks from cross-sector reliance on new or emerging trends in technology, energy

production, or sector-specific innovations that potentially increase the attack surface for critical infrastructure.

If the sector-specific strategies and sector-specific plans do not align with the strategic guidance issued by the Secretary of Homeland Security, DHS shall coordinate with SRMAs to resolve any differences, and, as necessary, elevate disagreements to the National Security Council staff.

Systemically Important Entities

The National Coordinator shall regularly identify organizations that own, operate, or otherwise control critical infrastructure that is prioritized based on the potential for its disruption or malfunction to cause nationally significant and cascading negative impacts to national security (including national defense and continuity of Government), national economic security, or national public health or safety. This list of Systemically Important Entities (SIE) shall be informed by inputs received from SRMAs and other Federal departments and agencies as appropriate, based on their respective sector-specific risk assessments, the cross-sector risk assessment, and other relevant critical infrastructure data -- including submissions of specific organizations from SRMAs for inclusion in the SIE list. This list of SIE shall be developed in coordination with SRMAs, and in consultation with other relevant Federal departments and agencies and other non-Federal entities, as appropriate. The list will not be made available to the public.

The SIE list shall inform prioritization of Federal activities, including the provision of risk mitigation information and other operational resources to non-Federal entities. The list of SIE developed pursuant to this memorandum, as well as any updates to

the list, will satisfy the requirement for the Secretary of Homeland Security to develop the list described in section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity). Where appropriate, regulators will consider this list when applying adequate risk management requirements.

Scope of Effort

Departments and agencies recognize that critical infrastructure is often interconnected globally and shall, as applicable, consider dependencies and interdependencies with assets, systems, and networks outside the United States as a part of sector risk management processes. Departments and agencies shall also collaborate with private-sector partners; State, local, Tribal, and territorial entities; foreign governments; international partners; and other entities that can take actions that provide resilience and security benefits to critical infrastructure owners and operators in the United States and globally. This effort shall include supporting sector coordinating councils, including the State, Local, Tribal, and Territorial Government Coordinating Council. These councils should be inclusive and include owners and operators, their trade associations, and other industry representatives.

Intelligence Sharing and Information Exchange

Critical infrastructure risk management requires those who own or operate infrastructure to be informed of a wide range of threats that are manmade or result from natural hazards, including by the actionable and timely intelligence and information available on those threats or hazards. To establish a comprehensive, integrated threat picture for United States critical infrastructure, the DNI

shall lead IC efforts, in consultation with DHS, including the National Coordinator, SRMAs, and relevant departments and agencies, to:

1. Use applicable tools and authorities to collect, integrate, analyze, and share information from intelligence reporting, data, and assessments to understand and identify threats to critical infrastructure. This shall include prioritizing the issuance of intelligence reports and analysis on such threats at the lowest possible classification level, consistent with the protection of sources and methods, such as through the robust use of tearlines, and, in coordination with SRMAs, disseminating intelligence reports in an accessible, useable, and shareable format for State, local, Tribal, and territorial governments, and owners and operators.

2. Leverage DHS and SRMA Priority Intelligence Requirements to inform collection and intelligence assessments related to threats to critical infrastructure in accordance with National Security Memorandum 12 of July 12, 2022 (The President's Intelligence Priorities), or any successor document, and the associated National Intelligence Priorities Framework (NIPF).

3. Coordinate with DHS, SRMAs, and other relevant Federal departments and agencies; State, local, Tribal, and territorial governments; and the private sector to enhance stakeholder and IC understanding of relevant threats to critical infrastructure and, where appropriate, integrate

sector risk perspectives into IC analysis.

4. Produce, receive, integrate, and share information, to include information from intelligence assessments and warnings, that enables Federal department or agency leadership to consider the widest possible options for mitigating a risk or addressing a threat, including the coordinated balancing of national interests, stakeholder equities, and authorities.

5. Share information with regulatory agencies, as appropriate, regarding threats to critical infrastructure to ensure they are aware of such threats, consistent with the protection of sources, methods, and investigations.

6. In coordination with DHS and DOJ, the DNI shall establish a process to ensure that IC elements provide, to the maximum extent possible, timely notification to appropriate Federal elements, including the FBI, CISA, and relevant SRMAs, when IC elements are aware of specific and credible threats to United States critical infrastructure. This process shall be implemented in a manner consistent with the protection of sources and methods; investigations; Executive Order 12333 of December 4, 1981 (United States Intelligence Activities); Executive Order 13636; applicable IC directives (including ICD-191); and authorities of the IC and its elements, as well as DHS, including title 6 and title 50 of the United States Code. Federal agencies receiving such information from the

IC shall, to the maximum extent possible and in a manner consistent with applicable agency authorities and investigative equities, promptly convey threat warnings to the targeted entities.

All departments and agencies, including the IC, shall coordinate with the National Coordinator and SRMAs designated in this memorandum, as appropriate, on outreach to entities within SRMAs' respective sectors to inform sector and cross-sector risk management and convey threat warnings. Collection and analysis of threats to critical infrastructure shall be informed by the President's Intelligence Priorities Framework and further prioritized and coordinated through the NIPF.

CISA shall also facilitate and share information and analysis to support Federal, State, local, Tribal, territorial, and private sector entities actions against all threats and hazards to critical infrastructure, including as the Federal civilian interface for the multi-directional and cross-sector sharing of information, particularly information related to cyber threat indicators, defensive measures, and cybersecurity risks. The SRMAs shall also share and receive information directly from owners and operators in their respective sectors. Information or intelligence shared with the self-organized and self-governed councils -- commonly referred to as sector coordinating councils -- comprised of a sector's owners and operators, trade associations, and other industry representatives, should be shared through or in coordination with a sector's respective SRMA.

Departments and agencies shall abide by all pertinent legal and policy procedures and use all appropriate legal and policy mechanisms to protect proprietary and sensitive commercial and

business information, as well as sensitive intelligence sources, methods, and activities.

Designated Critical Infrastructure Sectors and SRMAs

This memorandum identifies 16 critical infrastructure sectors and designates associated SRMAs. In some cases, co-SRMAs are designated where multiple departments share the roles and responsibilities of the SRMA. The Secretary of Homeland Security shall periodically evaluate the need for and approve changes to critical infrastructure sectors, and shall make recommendations to the President in accordance with statute and in consultation with the Assistant to the President and Homeland Security Advisor. The sectors and SRMAs are as follows:

Chemical:
Sector Risk Management Agency: DHS

Commercial Facilities:
Sector Risk Management Agency: DHS

Communications:
Sector Risk Management Agency: DHS

Critical Manufacturing:
Sector Risk Management Agency: DHS

Dams:
Sector Risk Management Agency: DHS

Defense Industrial Base:
Sector Risk Management Agency: DOD

Emergency Services:
Sector Risk Management Agency: DHS

Energy:
Sector Risk Management Agency: DOE

Financial Services:
Sector Risk Management Agency: Department of the Treasury

Food and Agriculture:
Co-Sector Risk Management Agencies: Department of Agriculture and Department of Health and Human Services (HHS)

Government Services and Facilities:
Co-Sector Risk Management Agencies: DHS and GSA

Healthcare and Public Health:
Sector Risk Management Agency: HHS

Information Technology:
Sector Risk Management Agency: DHS

Nuclear Reactors, Materials, and Waste:
Sector Risk Management Agency: DHS

Transportation Systems:
Co-Sector Risk Management Agencies: DHS and Department of Transportation

Water and Wastewater Systems:
Sector Risk Management Agency: Environmental Protection Agency

Implementation of This Memorandum

Except where otherwise directed by existing National Security Memoranda or Executive Orders:

1. Within 30 days of the date of this memorandum, SRMAs shall identify a senior leader who will serve as the primary representative to sectoral stakeholders for each respective sector and the day-to-day Coordinator of the SRMA Function.

2. Within 45 days of the date of this memorandum, the Secretary of Homeland Security shall issue strategic guidance that provides national-level priorities and a format that SRMAs shall use in the development of their sector-specific risk assessments and sector-specific risk management plans.

3. Within 180 days of the date of this memorandum, SRMAs, in coordination with the National Coordinator, shall develop plans to execute the required roles and responsibilities of each SRMA to ensure a continuity of effort and the coordination of policy and resourcing requirements. The plans should detail how the identified senior leaders will have the sufficient expertise, support capacity, and access to resources to consistently execute the roles and responsibilities of an SRMA. Plans should include potential colocation options; an assessment of the current structure; detailee arrangements between DHS, SRMAs, and the IC; and other potential maturity models. The National Coordinator, SRMAs, and other Federal departments and agencies shall, as appropriate, also establish personnel exchanges via Memoranda

of Understanding in order to develop subject matter expertise, interagency familiarity, and routine cross-pollination.

4. Within 1 year of the date of this memorandum, DHS, through CISA, shall officially establish or designate an office of the National Coordinator to serve as the single coordination point for SRMAs across the Federal Government. This office shall be distinct from the elements of CISA that carry out its SRMA functions and shall work with SRMAs to perform the duties of the National Coordinator, including managing the production of cross-cutting assessments, guidance, recommendations, and other priorities related to areas of significant cross-sector risk such as climate change, and DCI. It shall also manage the process to identify and support systemically important entities. This office shall also support SRMAs, as they work to execute the roles and responsibilities outlined in this memorandum, using DHS resources and authorities to help execute identified activities and achieve sector-level performance objectives, as appropriate. To the extent practicable, SRMAs will consider detailing sector-specific experts to this office for limited periods of time to enhance the national unity of effort. Alternatively, the National Coordinator will consider detailing representatives to SRMAs.

5. Within 270 days of the date of this memorandum, and on a recurring basis biennially by February 1 of each year, each SRMA shall submit its sector-specific risk management plan to

the Secretary of Homeland Security, based on guidance developed by DHS, through their Secretary or Agency Head. The plan shall be informed by the sector-specific risk assessment included as an annex. Each SRMA shall conduct a preliminary interim sector-specific risk assessment for the initial 270-day deliverable, and, on a biennial basis thereafter, a more complete and robust risk assessment. For the first sector-specific risk assessment and risk management plan cycle, draft sector-specific risk assessments will be provided to the National Coordinator within 180 days of the date of this memorandum to inform the first cross-sector risk assessment.

6. Within 1 year of the date of this memorandum, and on a recurring basis every 2 years thereafter by June 30 of each year, the Secretary of Homeland Security shall submit to the President and the Assistant to the President and Homeland Security Advisor the National Plan for approval. This plan shall be informed by sector-specific risk assessments and the cross-sector risk assessment.

7. Within 270 days of the date of this memorandum, as a one-time report, SRMAs and the National Coordinator shall submit to the Assistant to the President and Homeland Security Advisor a review of the available authorities, incentives, and other tools to encourage and require owners and operators to implement identified sector-specific or cross-sector minimum security and resilience requirements. This review should focus on identifying the most critical gaps in the Federal

Government's capacity to require and enforce minimum security and resilience requirements for critical infrastructure. As a part of this one-time report, the National Coordinator and SRMAs should provide the Office of Management and Budget a legislative proposal for any necessary additional authorities or capabilities that could enable the implementation of these minimum security and resilience requirements for critical infrastructure.

8. Within 1 year of the date of this memorandum, the Secretary of Homeland Security shall review the existing Critical Infrastructure Partnership Advisory Council framework for adequacy and make proposed changes. This shall include sector coordinating council requirements.

9. Within 180 days of the date of this memorandum, and thereafter annually by September 30 of each year, the DNI, in coordination with the Secretary of Defense (acting through the Under Secretary of Defense for Intelligence and Security), the Director of the FBI, and the Secretary of Homeland Security (acting through the Under Secretary for Intelligence and Analysis), and in consultation with SRMAs, shall submit to the President an intelligence assessment on threats to United States critical infrastructure. The intelligence assessment shall be submitted to the President in classified form at the highest level of classification necessary to fully characterize the threats. Within 90 days of the intelligence assessment's publication, including the first issuance and those recurring annually, the DNI, in

coordination with the Under Secretary of Defense for Intelligence and Security on behalf of the Secretary of Defense, the Director of the FBI, and the Secretary of Homeland Security (acting through the Under Secretary for Intelligence and Analysis), shall submit to the President a classified version of this assessment for release to appropriately cleared United States critical infrastructure owners and operators and SRMAs, and, within 180 days of the intelligence assessment's publication, share an unclassified version of the assessment with Federal, State, local, Tribal, territorial, and private sector partners, to the maximum extent possible and consistent with the protection of sources and methods.

10. Within 1 year of the date of this memorandum, and thereafter annually by June 30 of each year, the DNI, in coordination with IC elements, shall submit to the President a report on intelligence collection against threats to United States critical infrastructure. The report will describe collection and reporting for the prior year, including (by classification level) quantity, quality, and collection type; identify any intelligence gaps and offer recommendations on how they can be remedied; and analyze the extent to which such collection addresses the current threat, the President's Intelligence Framework, and the NIPF, noting any opportunities for improvement.

11. Within 18 months of the date of this memorandum, and thereafter annually by June 30 of each year, the DNI, in

coordination with IC elements, shall submit to the President a report on intelligence and information sharing on threats to United States critical infrastructure with owners and operators and SRMAs. The report will describe, at a strategic level, intelligence and information sharing for the prior year by all IC elements with those entities. This will include summaries of the information sharing between each IC element and other departments and agencies; infrastructure sector(s), including owners and operators; types of content shared (e.g., verbal briefing, written product, such as a tearline, etc.); and classification levels. The report also will identify any barriers to sharing and offer recommendations on how they can be remedied; assess the extent to which the process for reviewing requests for downgrades is effective and efficient; and evaluate the degree to which sharing in the reporting period addresses the requirements of this memorandum and the 2023 National Intelligence Strategy (or their successor documents), as well as any opportunities for improvement.

12. The DNI, the Secretary of Homeland Security, and SRMAs shall maximize the efficiency and effectiveness of United States Government engagements with critical infrastructure owners and operators by ensuring they are coordinated and deconflicted, consistent with agencies' authorities, third-party agreements, and protection of sources and methods. To accomplish this, the DNI and the Secretary of Homeland Security shall jointly develop, within 180 days of the date of this memorandum, policies, procedures, and guidance to ensure, respectively, the full participation of SRMAs and IC elements in ensuring this outcome. Not later than 180 days

after the completion of these guidance documents, the DNI shall institute an organizational approach, to include establishing or designating existing IC offices or elements, for coordinating the tracking of its engagements and information sharing with critical infrastructure owners and operators, and improve centralized reporting on these IC engagements, consistent with the protection of sources and methods and third-party agreements. The organizational approach should specify minimum tracking requirements, such as engagements with SIE, the nature of the engagement, and the date, and what general categories of engagements are excluded from tracking because of sensitivities involving sources, methods, contracts, third-party agreements, and other considerations.

13. Within 12 months of the date of this memorandum, the DNI shall establish implementing guidance to ensure all IC elements, to the maximum extent possible, timely notify appropriate Federal departments and agencies, including the FBI, CISA, and relevant SRMAs, when IC elements are aware of specific and credible threats to United States critical infrastructure. This process shall be implemented in a manner consistent with the protection of sources and methods; investigations; Executive Order 12333; Executive Order 13636; applicable IC directives (including ICD-191); and authorities of the IC and its elements, as well as DHS.

Definitions

The term "critical infrastructure" has the meaning provided in

section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely 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 national security, national economic security, national public health or safety, or any combination of those matters.

The term "all threats, 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, but is not limited to: natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, supply chain disruptions to degrade critical infrastructure, and disruptive or destructive activity targeting critical infrastructure.

The term "resilience" means the ability to prepare for threats and hazards, adapt to changing conditions, and withstand and recover rapidly from adverse conditions and disruptions.

The term "Federal departments and agencies" means 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).

The term "national security systems" means those systems as defined as NSS in 44 U.S.C. 3552(b)(6), as well as all other DOD and IC systems, as described in 44 U.S.C. 3553(e)(2) and 3553(e)(3).

The term "Sector Risk Management Agency" has the meaning provided in Public Law 117-263 (6 U.S.C. 650), namely a Federal department or agency, designated by law or Presidential directive, with

responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all-hazards environment in coordination with DHS.

The term "Federal Mission Resilience" means, as defined by the Federal Mission Resilience Strategy, the ability of the Federal executive branch to continuously maintain the capability and capacity to perform essential functions and services, without time delay, regardless of threats or conditions, and with the understanding that adequate warning of a threat may not be available.

The term "cross-sector" means relationships and interdependencies between critical infrastructure sectors that necessitate integrating and coordinating security and resilience activities.

The term "Defense Critical Infrastructure" means DOD and non-DOD networked assets and facilities essential to project, support, and sustain military forces and operations worldwide. Non-DOD owned Defense Critical Infrastructure consists of assets from relevant critical infrastructure sectors and subsectors, including as defined by statute.

The term "supply chain" refers to a linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

The term "risk assessment" is defined as risk identification, analysis, and evaluation, designed to inform risk management.

The term "assets" means a person, structure, facility, information, material, equipment, network, or process, whether physical or virtual, that enables an organization's services, functions, or capabilities.

The term "criticality" means an attribute of an asset, system, or service that reflects its degree of importance or necessity to stated goals, missions or functions, or continuity of operations as they apply to national security (including national defense and continuity of Government), national economic security, or national public health or safety.

The term "sector" means a collection of assets, systems, networks, entities, or organizations that provide or enable a common function for national security (including national defense and continuity of Government), national economic security, national public health or safety, or any combination thereof.

The term "subsector" means a subset of a sector comprised of critical infrastructure grouped by common resources, common equities, or common functions.

The term "systems" means a combination of personnel, structures, facilities, information, materials, equipment, networks, or processes, whether physical or virtual, integrated or interconnected for a specific purpose that enables an organization's services, functions, or capabilities.

The term "intelligence" has the meaning provided in the National Security Act of 1947, as amended.

The term "intelligence sharing" in the context of this memorandum

refers to the timely sharing of intelligence, including credible and specific threat information, assessments, data, or analysis for the purpose of enhancing overall United States national and homeland security and resilience, in accordance with applicable classification handling and intelligence sharing policies and procedures.

The term "information sharing" in the context of this memorandum refers to the bi-directional sharing of timely and relevant information concerning risks to United States critical infrastructure. In the context of this memorandum only, intelligence sharing is an element of information sharing.

The terms "coordinate" and "in coordination with" mean a consensus decision-making process in which the named coordinating department or agency is responsible for working with the affected departments and agencies to achieve consensus and a consistent course of action.

The term "collaboration" means the process of working together to achieve shared goals.

The term "national essential functions" means that subset of Government functions that are necessary to lead and sustain the Nation before, during, and in the aftermath of an emergency.

The term "primary mission essential functions" means those Government functions that must be performed in order to support or implement the performance of the national essential functions before, during, and in the aftermath of an emergency.

General Provisions

This memorandum rescinds and replaces Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

(a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or
(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.