Continuity of the Economy Response

Publication: August 17, 2023

Cybersecurity and Infrastructure Security Agency

The overall classification of this product is UNCLASSIFIED//FOR OFFICIAL USE ONLY.

Executive Summary

Introduction

In section 9603 of the National Defense Authorization Act for Fiscal Year 2021 (FY 2021 NDAA), Congress requires that "[t]he President shall develop and maintain a plan to maintain and restore the economy of the United States in response to a significant event." The FY 2021 NDAA defines "significant event" as "an event that causes severe degradation to economic activity in the United States due to (A) a cyber attack; or (B) another significant event that is natural or human-caused." The FY 2021 NDAA lays out 19 requirements for the content of the plan.

In March 2022, Congress appropriated $200,000 to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) for this effort. Given the limited resources available and potential for overlap with existing authorities, policies, plans, and frameworks, the National Security Council (NSC) and the interagency reviewed and endorsed CISA's proposal to develop a response to the Continuity of the Economy (COTE) requirement ("the COTE response") that analyzes the specific requirements in the legislation; provides an initial review of where those requirements may be addressed by existing federal government authorities, policies, plans, and frameworks; identifies gaps and makes recommendations on a path forward to ensure economic recovery is addressed in response efforts.

CISA prepared the COTE response using United States (U.S.) government policies, analysis, authorities, frameworks, published reports, news articles, and academic studies. CISA also consulted with other federal departments and agencies, private sector entities, and non-governmental and international organizations to brief them on COTE concepts and to gain their insights on this important matter.

Key Finding and Recommendations

The U.S. maintains a robust architecture of authorities, policies, plans, and frameworks for Federal Mission Resilience and domestic incident preparedness, response, and recovery. The goal of maintaining and restoring the U.S. economy in response to a significant event is fundamentally embedded into many components of this architecture.

The key finding of the COTE response is that, broadly, COTE plan requirements included in the FY 2021 NDAA are addressed through existing authorities, policies, plans, and frameworks. Creation of a COTE plan with a singular economic focus, coupled with new response frameworks, has the potential to create confusion and duplicate existing response and recovery mechanisms. However, the fundamentally important concept of economic recovery and response detailed in the COTE requirement should be deeply integrated within existing incident response frameworks to avoid creating an additional layer of potentially divergent planning and response activities operating in parallel to already established procedures. In lieu of developing a standalone COTE plan, the federal government should continue to refine and strengthen existing authorities, policies, plans, and frameworks for Federal Mission Resilience and domestic incident preparedness, response, and recovery. This COTE response provides several specific recommendations for how the federal government can continue to enhance the ability to maintain and restore the U.S. economy in response to a significant event.

1. Recommendations for Further Analysis to Identify Gaps

1.1 Continue to Analyze Existing Critical Infrastructure Dependencies and Interdependencies Data.

Critical infrastructure sectors are dependent on one another and a disruption in one sector is increasingly felt across other sectors, broadening the array of impacts that may result from a significant event. To confirm that existing plans and policies address the full range of cascading impacts, CISA recommends

that sectors, through the Sector Risk Management Agencies (SRMAs), review existing risk assessments to better understand the concentrated dependencies and potential risk vectors across the sectors from an economic perspective and determine if there are any gaps relating to economics in their plans.

1.2 Ensure Routine Review of Existing Authorities, Policies, Plans, and Frameworks to Confirm Inclusion of Economic Impacts.

To support development of the COTE response, CISA conducted an initial analysis of how specific FY 2021 NDAA requirements for a COTE plan are already addressed by existing federal government authorities, policies, plans, and frameworks. This initial analysis should be reviewed, validated, and confirmed by federal agencies as part of their regular update cycles to determine if there are any gaps in coverage of economic recovery issues.

There is significant alignment between the response priorities to protect life and restore services and those actions needed to ensure continuity of the economy. To ensure that all specific requirements of the FY 2021 NDAA are addressed, CISA recommends the initial gap analysis conducted for this COTE response be expanded by working with federal agencies, including the SRMAs of critical infrastructure sectors, state, local, tribal, and territorial (SLTT) governments, and broader communities of interest to review existing National Planning Frameworks and specific policy frameworks that apply to individual sectors. The goal of the expanded gap analysis is to identify where unique planning and response activities may be needed to ensure continuity of the economy is accounted for in existing plans and frameworks.

2. Recommendation to Scope Requirements

CISA provides the following recommendation to scope the requirements of the FY 2021 NDAA:

2.1 Initially Prioritize Seven Key Critical Infrastructure Sectors.

To support development of the COTE response, CISA identified seven key priority critical infrastructure sectors for focus when reviewing plans and procedures. This determination is based on research, interagency and private sector stakeholder discussions, survey responses, and advice from subject matter experts. The seven key critical infrastructure sectors are: Energy, Communications, Information Technology, Financial Services, Food/Agriculture, Transportation, and Water/Wastewater. These priority sectors should be validated and updated via existing risk management forums and councils after the further analysis called for in Recommendations 1.1 and 1.2.

3. Recommendations to Plan and Prepare for Economic Restoration After a Significant Event

CISA recommends the following considerations to advance the overall capability to plan and prepare for economic restoration. These recommendations can be addressed under existing federal government authorities, policies, plans, and frameworks.

3.1 Develop A Risk-Based Approach Using Planning Scenarios.

CISA recommends federal agencies create a set of economic-focused planning scenarios to aid both the development of the expanded gap analysis (Recommendation 1.1) and the response to a significant event as a part of their routine planning and analysis efforts. Utilizing data and insights from public and private stakeholders to establish a risk-based approach using planning scenarios based on economic impacts would assist in building resilience prior to an incident and support decisions on prioritization and reconstitution of the economy post-event. Adapted for continuity of the economy planning, global economic risk and dependency analysis and consequence modeling could identify scenarios that may cause national-level degradation to National Critical Functions (NCFs) and the proposed seven key critical infrastructure sectors identified for initial analysis.

3.2 Define Data Needs to Support Economic Restoration.

Currently, there are numerous federal data collection efforts and existing frameworks relevant to continuity of the economy across the interagency. CISA recommends following on the work of Recommendation 1.1 by better defining the data that would be most valuable for economic restoration.

Requirements A-S Recommendations

The COTE response also provides analysis of Requirements A-S, as detailed in the FY 2021 NDAA. CISA provides recommendations for additional analysis to help scope 11 of the 19 requirements that agencies and sectors can utilize to enhance any routine planning efforts.

TABLE OF CONTENTS

Executive Summary i

1. Introduction 1

2. Methodology 1

3. Analysis 2

3.1 Analysis: Stakeholder Feedback Themes 2
3.2 Analysis: Relationship of COTE to Existing Emergency Preparedness and Response Policies, Processes, and Frameworks 3
3.3 Analysis: Relationship of the COTE to Other Relevant Authorities 8
3.4 Recommendations for Further Analysis to Identify Gaps 13
3.5 Recommendation to Scope Requirements 14
3.6 Recommendations to Plan and Prepare for Economic Restoration After a Significant Event 15
3.7 Analysis: Assessment of COTE Requirements A-S 16

1. Introduction

In section 9603 of the National Defense Authorization Act for Fiscal Year 2021 (FY 2021 NDAA), Congress requires that "[t]he President shall develop and maintain a plan to maintain and restore the economy of the United States in response to a significant event." The FY 2021 NDAA defines "significant event" as "an event that causes severe degradation to economic activity in the United States due to (A) a cyber-attack; or (B) another significant event that is natural or human caused." The FY 2021 NDAA lays out 19 requirements for the content of the plan.

In March 2022, Congress appropriated $200,000 to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) for this effort. Given the limited resources available and the potential for overlap with existing authorities, policies, plans, and frameworks, the National Security Council (NSC) and the interagency reviewed and endorsed CISA's proposal to develop a response to the Continuity of the Economy (COTE) requirement ("the COTE response") that analyzes specific requirements in the legislation; provides an initial review of where those requirements may be addressed by existing federal government authorities, policies, plans, and frameworks; identifies gaps and makes recommendations on a path forward to ensure economic recovery is addressed in response efforts.

The key finding of the COTE response is that, broadly, COTE plan requirements included in the FY 2021 NDAA are effectively addressed through existing authorities, policies, plans, and frameworks. Creation of a COTE plan with a singular economic focus coupled with new response frameworks, has the potential to create confusion and duplicate existing response and recovery mechanisms. However, the fundamental concept of economic recovery and response detailed in the COTE requirement should be deeply integrated within existing incident response frameworks to avoid creating an additional layer of potentially divergent planning and response activities operating in parallel to established procedures. In lieu of developing a standalone COTE plan, the federal government should continue to refine and strengthen existing authorities, policies, plans, and frameworks for Federal Mission Resilience and domestic incident preparedness, response, and recovery.

CISA developed the following recommendations as a path forward to continue to improve and strengthen the architecture to maintain and restore the U.S. economy in response to a significant event. Given that most critical infrastructure is owned and operated by the private sector, and that assets reside within jurisdiction of state, local, tribal, and territorial communities, outreach beyond the federal enterprise will be required to execute all recommendations.

2. Methodology

CISA utilized a multi-faceted approach for developing the COTE response including open-source research and data collection along with extensive interagency and private sector stakeholder engagement to educate stakeholders of the COTE plan mandate and obtain their insights, feedback, and appropriate data. CISA assessed COTE concepts and the 19 COTE requirements through a consideration of relevant authorities, frameworks, statutes, government reports, stakeholder interviews, survey responses from over twenty agencies and Sector Coordinating Councils, academic literature, news reports, and articles.

This document:

- Evaluates the 19 requirements of the COTE against existing policies, authorities, literature, data, plans, and frameworks to determine how requirements may already be addressed.
- Identifies requirements that may be outside the COTE scope.
- Assesses data for completeness and identifies methods for collecting and validating data that can be used by stakeholders as they continue to integrate economic response and recovery issues in the normal course of planning and response assessments.
- Assesses capabilities and response efforts that exist to respond to a significant COTE type event.

This COTE response can serve as a resource for federal departments and agencies as they review existing authorities, policies, plans, and frameworks to determine if there are any gaps in the coverage of economic response and recovery planning. This document applies proven methodologies, frameworks, international risk standards, and analysis that can help departments and agencies understand how to approach this complex issue. The response also identifies relevant data gaps and highlights adjacent policies, frameworks, and authorities.

The COTE response provides an actionable approach for the federal government and industry to continue to integrate economic continuity and restoration matters into existing policies, processes, plans, or frameworks.

3. Analysis

Recommendations for the COTE response are informed by the following analysis:

3.1 Analysis: Stakeholder Feedback Themes

CISA gathered feedback through interviews and responses to written due diligence questions from public and private sector partners. CISA received over two dozen responses; the section below highlights the major themes garnered from the provided input:

1. Government and private sector respondents indicate a widely agreed upon definition of a "significant event" does not exist, although individual communities have definitions relevant to their sector.

- Respondents indicate that significant events can be from man-made or natural causes, in addition to planned or accidental causes. Respondents indicate a significant event that "causes catastrophic damage" to their respective infrastructure would have the following characteristics: (1) require an extended period to restore, (2) degrade their ability to provide routine services in key critical infrastructure sectors, (3) cause damage that is beyond the capacity of existing supply chains to restore–all of which would make their respective sectors inoperable.

2. A majority of government and private sector respondents have preparedness plans in place to support a response to a major event.

- Almost all respondents–including both government and private sector–indicate they have resilience or emergency response plans in place that are relevant to significant events. Like the priority lists, these resilience and emergency response plans generally only pertain to the specific sector and there are few instances of comprehensive resilience plans, except for continuity of operations (COOP) and continuity of government (COG) planning. For example, private sector respondents note that some sector-specific emergency or disaster management response plans are restricted to loss of, or damage to, a facility, key supplier, or critical resource rather than a loss of overall infrastructure.

3. Some respondents believe that emergency services and first responders are essential for the safety/security of personnel and goods in key critical infrastructure sectors.

- Some private sector respondents indicate that it is critically important for there to be emergency services and first responders available during a significant event, including law enforcement and medical personnel. Respondents note that these services are essential for ensuring the safety, security, and health of personnel who are charged with restoring power, telecommunications, transportation, water management, and other critical infrastructure needs in a significant event. Furthermore, the safety and security of goods, such as fuel and other critical materials, and transportation of such goods is essential during a significant event. One respondent emphasized that private sector groups have–and will–compete over limited supplies of construction materials, generators, fuel, and disaster service teams; therefore, the safety and security of such items is critical for immediate response and recovery.

4. A consensus exists among respondents about the top critical infrastructure sectors to bring back online prior to any others.

- Respondents believe that the following critical infrastructure sectors must be brought back online before all others: Energy, Communications, Transportation, Water and Wastewater, and Information Technology.

3.2 Analysis: Relationship of COTE to Existing Emergency Preparedness and Response Policies, Processes, and Frameworks

In Table 1 below, CISA assessed key emergency preparedness and response policies, processes, and frameworks currently utilized by both the government and private sector to determine if they are applicable or duplicative to the COTE requirement. Among other frameworks, key frameworks discussed below include Presidential Policy Directives (PPD) 8 and 21, the National Response Framework, the National Essential Functions structures and related frameworks and highly relevant sub-elements. Together, these policies serve as the backbone for current incident response planning and operations and are critical to coordinating government actions responding to a significant incident.

Many of these policies, processes, and frameworks focus primarily on emergency life-safety response and recovery, while the COTE focuses exclusively on the economy. However, these approaches are inherently intertwined as economic recovery cannot happen without the emergency and recovery response, and long-term sustainability of response and recovery operations relies on a functioning economy.

Table 1: Representative Emergency Preparedness and Response Policies, Processes, and Frameworks

Document	Description	Impact	Relevancy to COTE	Maturation and Review: Potential Gaps
Presidential Policy Directive – 21 (PPD-21), Critical Infrastructure Security and Resilience	Establishes national policy on critical infrastructure security and resilience, advancing a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.	Critical infrastructure security and resilience is a shared responsibility among the federal, SLTT entities, public and private owners and operators of critical infrastructure. Clarifies the critical infrastructure-related functions, roles, and responsibilities across the federal government.	Establishes policy on security and resilience of critical infrastructure sectors, specifically identifying 16 sectors and associated SRMAs. Efforts to ensure security and resilience of critical infrastructure also support continuity of the economy.	Although PPD-21 requires, among other responsibilities, the Secretary of Homeland Security to coordinate federal government response to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities, it does not provide additional detail (and is not focused exclusively on significant events as described in this document). It is designed to proactively strengthen critical infrastructure and manage risks against physical and cyber threats. It considers all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. The National Security Council is currently facilitating a process to review and revise, as appropriate, PPD-21.
National Critical Functions (NCFs)	Functions of government and the private sector so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on national and/or economic security, public health, or safety.	Allows for a more robust prioritization of critical infrastructure and a systematic approach to corresponding risk management activity.	Utilized to support disaster-specific response and restoration operations. NCFs could serve as a foundation for COTE infrastructure models or analysis of dependencies and interdependencies.	Framework for creating replicable, rapid analysis applicable to economic functions provided by infrastructure. NCFs can be, and more frequently are, applied to events that are more broadly defined than a significant event.
National Critical Infrastructure Prioritization	Prioritizes critical infrastructure assets based on consequences	CISA identifies a list of systems and assets that would cause, among other things, national or regional	NCIPP provides a list of critical assets that response and recovery activities could protect or distribute products from or to and identifies	NCIPP participation by SLTT entities is voluntary and implemented with varying thoroughness, limiting the broad infrastructure view needed by

Document	Description	Impact	Relevancy to COTE	Maturation and Review: Potential Gaps
Program (NCIPP)	associated with disruption or destruction.	catastrophic effects. CISA annually updates and prioritizes the list.	what assets could be impacted by significant events.	planners. Full NCIPP list is classified, which restricts usage.
Presidential Policy Directive-8 (PPD-8), National Preparedness	Aimed at strengthening national security and resilience. through preparation for threats that pose the greatest risk to the security of the nation.	Calls on federal departments to work with the whole community around six elements: A common goal; an organized approach; national planning frameworks in five mission areas (prevention, protection, mitigation, response, and recovery); annual reporting; and state and federal plans	Addresses resilience and preparation for any type of threat or hazard and could potentially include an incident that would rise to level of a significant event.	Does not specifically address recovery of the economy, but operational plans that are developed under the National Preparedness Goal do address the impacts to and resilience of the economy and post-disaster recovery of the economy.
National Response Framework (NRF)	Guide to how the nation responds to all types of disasters and emergencies. The structures, roles, and responsibilities can be partially or fully implemented in context of a significant event.	Provides structure and process for current domestic response activities. NRF includes Emergency Support Functions that provide structure for coordinating federal interagency support for a federal response to an incident.	Specifies that at the national level, a catastrophic incident is one of such extreme and remarkable severity or magnitude that the nation's collective capability to manage all response requirements would be overwhelmed.	Does not focus on economic recovery. The NRF applies to all incident types, to include COTE-type events. The NRF structure is frequently activated for regional or smaller events that do not require significant economic restoration but can apply to larger incidents, if required.
FEMA's Community Lifelines [related to PPD-8 and the NRF]	Constructed to increase effectiveness in disaster operations and better position the agency to respond to catastrophic incidents.	During initial response, efforts focus on stabilizing community lifelines which provide an outcome-based, survivor-centric frame of reference that assists responders.	The Community Lifelines Toolkit 2.0 provides a one-stop-shop for information on construct of lifelines, components and sub-components of lifelines, key questions in an emergency, and analysis process.	This is limited to an incident with significant life and safety impacts. A COTE type response would focus not only on a disaster framework but would consider other incidents that constitute a significant event.
Emergency Support Function (ESF)-14 – Cross Sector Business and Infrastructure	Provides a mechanism to align and support cross-sector operations among infrastructure owners and operators, businesses, and government partners	Supports efforts to enable collaboration and coordination among critical infrastructure sectors and helps coordinate and sequence operations to mitigate cascading failures and risks. Integrates SRMA	Supports deliberate planning by identifying critical nodes among infrastructure sectors; assessing potential single points of failure in NCFs and supply chains; provides analysis to support integrated cross-sector response planning by	Excludes economic policymaking. The National Economic Council, the Council of Economic Advisors, and the Department of Treasury develop all national economic stabilization policy outside of the ESF-14 structure. ESF-

Document	Description	Impact	Relevancy to COTE	Maturation and Review: Potential Gaps
[related to PPD-8 and the NRF]	to stabilize community lifelines, as well as any impacted NCFs.	incident response operations with ESFs and public-private sector coordinating entities.	infrastructure owners and operators, and SLTTs.	14 is newest ESF and is developing processes and deliverables.
National Essential Functions (NEFs)	Select functions of the executive branch that are necessary to lead and sustain the Nation during a catastrophic emergency.	NEFs are the foundation of all continuity programs and capabilities.	Maintaining a stable economy (NEF 7) underpins the notion of continuity of the economy.	The executive branch continuity programs that support NEFs are focused on ensuring that the essential functions of the federal executive branch are performed continuously regardless of circumstance.
Homeland Security Presidential Directive-5 (HSPD-5)	Establishes a single, comprehensive national incident management system.	Aligns with the Homeland Security Act and makes the DHS Secretary the principal federal official responsible for coordinating preparedness activities and operations within the United States to respond to and recover from terrorist attacks, major disasters, and other emergencies. Requires creation of the National Incident Management System (NIMS).	Requires the DHS Secretary to coordinate federal government response operations under certain circumstances.	It may not be clear how NIMS and/or the principal federal official role of the Secretary could be used to coordinate the economic consequences of a significant event.
Presidential Policy Directive-44 (PPD-44)	Provides a process for timely identification of a lead federal agency (LFA) when there is neither a presidential declaration under the Stafford Act nor clear federal roles and responsibilities pertaining to incident response.	Addresses identified need to enhance federal government's response to domestic incidents.	PPD-44 could potentially be used to establish an LFA for the response to a significant event.	LFAs are identified in PPD-44 based on their underlying authorities. There may not be clear, existing authorities for departments and agencies to manage a significant event with widespread impacts, making it difficult to identify who the single LFA would potentially be.
Presidential Policy Directive-41(PPD-41)	Principles governing response to any public or private sector cyber incident. For	Guidance for cyber asset response, threat response, and intelligence activities and provides unity of effort	Would guide federal government response to the cyber aspects of a significant event.	While the document proposes mechanisms to align the coordination structure of PPD-41 with other coordination lines of effort occurring

Document	Description	Impact	Relevancy to COTE	Maturation and Review: Potential Gaps
	significant cyber incidents, establishes LFAs and architecture for coordinating broader federal government response.	amongst federal government through national policy and operational coordination.		contemporaneously under other authorities, this approach has not been executed to sufficiently evaluate potential implementation challenges.

3.3 Analysis: Relationship of the COTE to Other Relevant Authorities

CISA took a comprehensive and holistic approach to assessing relevant current authorities both preparing for, and responding to, a significant event in order to determine if they are applicable or duplicative to the COTE requirement. In some cases, the reviewed authorities in Table 2 underpin frameworks discussed in Table 1. The review in Table 2 below includes examining the most prominent authorities available to the executive branch, including its independent departments and agencies and includes: (1) authority for the COTE plan as it relates to other existing plans and authorities; (2) authorities available to coordinate, supervise, and direct the Whole-of-Government response to a significant event; and (3) operational authority of federal government departments and agencies to respond to a significant event.

Table 2: Representative Relevant Authorities

Authority	Description	Impact	Relevancy to COTE	Status	Potential Gaps
Robert T. Stafford Disaster Relief and Emergency Assistance Act	Establishes a federal process for declaring disasters and defines the scope of disasters from emergency to major disaster. Outlines the approach to providing resources for a response, authorizes federal assistance programs, and articulates need for state and local governments to create comprehensive disaster preparedness plans and build capabilities.	Authorizes President to provide financial and direct federal assistance to state and local governments, private nonprofit organizations, and individuals to support response, recovery, and mitigation efforts following Presidential emergencies or major disaster declarations.	Authorizes federal government to aid states and local governments during a declared emergency or major disaster (which may also qualify as a significant event as defined in this COTE response). Assistance includes food, shelter, financial assistance, and the repair of physical damage resulting from a disaster.	No Expiration	Depending on the facts specific to a particular incident, a significant event, as defined in the context of COTE, may or may not qualify as a "major disaster" or "emergency" under the Stafford Act. Also, the Stafford Act is not a primary source of economic recovery authorities.
Federal Power Act (FPA)	Primary federal statute governing the wholesale transmission and sale of electric power, as well as the regulation of hydroelectric power.[1]	FPA created the Federal Power Commission, which regulates construction and operation of nonfederal hydropower projects. Created an independent commission that can grant licenses that permit private and municipal developers to construct and operate hydropower projects.	Addresses several issues related to Energy sector, including electric power and reliability.[2] Also addresses "cybersecurity protection" and defines "cybersecurity incident"[3], which could fall under the definition of significant event.	No Expiration	Does not specifically address economic recovery. FPA provisions exist in steady-state environment, whereas authority needed to respond to significant event exceeds the bounds of steady-state operations and has not been tested in a significant event.
Public Health Service Act	Covers HHS legal authority for responding to public health emergencies and authorizes HHS to lead all federal public	Established federal government's quarantine authority and gave U.S. Public	Authorizes HHS to monitor and oversee federal public health and medical responses to public health emergencies under the	No Expiration	Provides broad authorities to respond to a declared public health emergency and to provide health and medical

[1] Congressional Research Service, "The Legal Framework of the Federal Power Act," January 22, 2020, https://crsreports.congress.gov/product/pdf/IF/IF11411.
[2] *Federal Power Act,* 16 U.S.C. §§ 791a et seq.
[3] "The term 'cybersecurity incident' means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."

Authority	Description	Impact	Relevancy to COTE	Status	Potential Gaps
	health and medical response to public health emergencies.	Health Service responsibility for preventing introduction, transmission, and spread of communicable diseases from foreign countries into U.S.[4]	NRF and declare and respond to public health emergencies. Assists states in addressing health emergencies; and maintains the Strategic National Stockpile.[5] A health emergency could also qualify as significant event, based on definition included in this report.		support to state and local governments but does not provide authority to respond to economic consequences of significant event affecting the critical infrastructure sectors.
Cybersecurity and Infrastructure Security Agency Act of 2018	Creates CISA and mandates that agency's responsibilities include leading cybersecurity and critical infrastructure security programs, operations, and associated policy.	Creates CISA to secure the nation's critical infrastructure and information technology systems that support them.	Variety of authorities and responsibilities that would be used to prepare for and support response to a significant event. Other authorities and responsibilities, such as those found in Presidential Policy Directive-41, U.S. Cyber Incident Coordination, potentially provide CISA a significant role in a significant event.	No Expiration	Provides responsibilities and direction to CISA to create several key capabilities to prepare and respond to cyber events and coordinate national critical infrastructure efforts that would be crucial to supporting economic recovery.
Defense Production Act of 1950 (DPA)	Confers upon the President a broad set of authorities to influence domestic industry in interest of national defense. The President has delegated authorities to department and agency heads in Executive Order 13603, National Defense Resource Preparedness.	Title I prioritizes government contracts and issues allocation orders. Title III offers incentives within domestic market when necessary for national defense. Title VII includes preparedness authorities that allows the Federal	Authorities extend beyond shaping U.S. military preparedness and capabilities, as the authorities may also be used to enhance and support domestic preparedness, response, and recovery. The DPA also provides the authority for reviews of foreign investments into U.S. companies that could pose national security concerns	Authorized through 9/30/25. Non-permanent provisions must be reauthorized or many authorities will terminate.[6]	Could provide the President another tool to guide nation's economy after significant event, if justified for national defense interests.

[4] U.S. Center for Disease Control and Prevention, *History of Quarantine*, National Center for Emerging and Zoonotic Infectious Diseases, Division of Global Migration and Quarantine, July 20,2020, https://www.cdc.gov/quarantine/historyquarantine.html.
[5] U.S. Department of Health and Human Services, *HHS Legal Authorities Related to Disasters and Emergencies*, June 16, 2021, https ://www.phe.gov/Preparedness/planning/authority/Pages/default.aspx.
[6] Federal Emergency Management Administration, *Defense Production Act*, https://www.fema.gov/disaster/defense-production-act

Authority	Description	Impact	Relevancy to COTE	Status	Potential Gaps
		Government to partner, plan and coordinate with the private sector.	which provides risk assessment and mitigation preventing outside influence on the economy.		
National Contingency Plan (NCP)	Provides organizational structure and procedures for preparing for and responding to discharges of oil and releases of hazardous substances, pollutants, and contaminants.	Primary source of coordination and authority for responding to significant event where it is wholly or partially based upon releases of hazardous substances, pollutants, and contaminants.	Primary source of coordination and authority for responding to significant event where it is wholly or partially based upon the releases of hazardous substances, pollutants, and contaminants.	No Expiration.	While the NCP is frequently in use, it is unclear how the NCP could align into a Whole-of-Government significant event response, where NCP activities are just one of several national lines of effort.
National Emergencies Act	Provides a framework for the exercise of emergency powers under other statutes.	The Act requires the President to follow certain procedures in order to utilize various "national emergencies" authorities set forth in provisions throughout the U.S. Code.	The purpose is to make additional authorities available to President and federal departments and agencies, some of which would be used to respond to significant event.	No Expiration	Does not specifically address economic recovery; however, for President to enable full authorities of federal government, a national emergency declaration must follow the procedures outlined in the Act.
Executive Order (EO) 12656	Assigns national security emergency preparedness responsibilities to federal departments and agencies to prepare and respond to a "national security emergency."	Penultimate order from President to align all major federal departments and agencies to be prepared to reorient focus of their capabilities to support Whole-of-Government response to national security emergency.	Provides off the shelf, readymade framework to organize preparing for a COTE type event as "national security emergency" is an earlier term for a significant event. Coupled with other authorities, provides an immediate authority to align COTE type preparedness efforts.	No Expiration	Departments and agencies specified have undergone reorganizations and renaming. Principles and duties have appeared in subsequent Presidential directives and statutory changes since the issuance of EO 12656.
Global Catastrophic Risk Management Act of 2022	Assigns authority to plan and prepare for global catastrophic and existential risk, to include report containing assessment of these risks, supplement each	Establishes long term planning and risk assessments for catastrophic risk and develops an	Directs FEMA and DHS to create a strategy to ensure the health, safety, and general welfare of the civilian population	No Expiration	Contemplates the most extreme levels of physical and economic degradation that would be termed a significant event under

Authority	Description	Impact	Relevancy to COTE	Status	Potential Gaps
	Federal Interagency Operational Plan with enhanced catastrophic incident annex, conduct exercise as part of national exercise program to test strategy, and report to Congress.	interagency strategy to enhance resiliency and plan to ensure the basic needs of the citizenry are met if critical infrastructure is destroyed or offline.	affected by catastrophic incidents.		COTE. Strategy and plans could conflict or be redundant to COTE if they are not part of an integrated planning and exercise process.

3.4 Recommendations for Further Analysis to Identify Gaps

CISA developed the following recommendations as a path forward to continue to improve and strengthen the architecture to maintain and restore the U.S. economy in response to a significant event.

3.4.1 Continue to Analyze Existing Critical Infrastructure Dependencies and Interdependencies Data

Critical infrastructure sectors are dependent on one another and a disruption in one sector is increasingly felt across other sectors, broadening the array of impacts that may result from a significant event. To prioritize recovery efforts, economic continuity planning should identify the critical nodes, dependencies, and interdependencies within national infrastructure that guarantee U.S. economic resilience.

RECOMMENDATION: To confirm that existing plans and policies address the full range of cascading impacts, CISA recommends that sectors, through the SRMAs, review existing risk assessments to better understand concentrated dependencies and potential risk vectors across the sectors from an economic perspective and determine if there are gaps relating to economics in their plans. Sectors should prioritize economic recovery gaps found in their plans and develop plans to stand up services for business and economic continuity.

As the SRMAs update their Sector Specific Plans during their regular review cycles, CISA can provide guidance for sectors regarding how they can factor economic impacts into their risk assessments as they highlight areas of greatest risk and how best to map to mitigation strategies. In addition, the federal government should ensure that economic recovery functions are taken into consideration in the planning and response phases of the Emergency Support Functions, Recovery Support Functions, and Support Annexes.

3.4.2 Ensure Monitoring of Existing Authorities, Policies, Plans, and Frameworks to Confirm Inclusion of Economic Impacts.

The COTE requirement complements a vast landscape of preparedness, response, and resilience authorities, policies, plans, and frameworks, which CISA analyzed for the COTE response. This initial analysis should be reviewed, validated, and confirmed by federal agencies as part of their regular update cycles to determine if there are any gaps in coverage of economic recovery issues.

CISA's understanding of the severity of a significant event is that it would prompt existing emergency response and continuity plans. There is significant overlap between the response priorities to protect life and restore security for those needed to ensure continuity of the economy. Based on our analysis, CISA concludes that there is significant alignment between the response priorities to protect life and restore services and those actions needed to ensure continuity of the economy.

While it appears that no one policy, process, response framework, or authority addresses all issues that pertain to an economic focus following a significant event, for further clarity, a governance and gap analysis should be performed on all policies, processes, frameworks, and authorities detailed in Table 1 and Table 2 above.

RECOMMENDATION: To ensure that all specific requirements of the FY 2021 NDAA are addressed, CISA recommends the initial gap analysis conducted for this COTE response be expanded by working with federal agencies, including the SRMAs of critical infrastructure sectors, as well as SLTT governments, and broader communities of interest to review existing National Planning Frameworks and specific policy frameworks that apply to individual sectors. The goal of the expanded gap analysis would be to identify where unique planning and response activities may be needed to ensure continuity of the economy activities are accounted for in existing plans and frameworks.

When aligning COTE objectives to existing authorities, policies, plans, and frameworks, federal agencies can identify implementation gaps that require guidance and elevate those findings to the administration

for potential action. A review of existing NRFs should be part of the gap analysis. The goal of the gap analysis is to identify unique planning and response activities needed to ensure continuity of the economy and those activities not already accounted for in existing plans such as ESF-14. Establishment of a cross-sector, cross-jurisdictional collaborative review group to identify gaps is critical.

Based on our research to date, CISA identified that NRF contains similarities to potential COTE-type functions. The NRF contains a definition of applicable incidents which could encompass COTE-type considerations and identifies robust processes and roles and responsibilities to effectively coordinate response activities. However, as noted previously, NRF is frequently activated for non-COTE level events and has not focused on economic restoration of a COTE-type event. ESF-14, which is an element within NRF, is intended to bridge public and private sector responses, allowing for coordinated response activity that expands beyond federal capabilities. This recently established organizing construct focused on critical infrastructure and shared activity has many of the appropriate stakeholders already within the target community. However, specific financial coordinated response activities have not previously been considered within ESF-14 activities and as such, economic considerations would need to be added to ESF-14.

Existing executive branch review processes and policy frameworks that include economic elements should consider items listed in the FY 2021 NDAA section 9603.a.3, as appropriate.

3.5 Recommendation to Scope Requirements

CISA provides the following recommendation to scope requirements of the FY 2021 NDAA:

3.5.1 Initially Prioritize Seven Key Critical Infrastructure Sectors

PPD-21 identifies the nation's 16 critical infrastructure sectors, all of which are critically important to our nation's economy and national security. During a significant event it is possible that some, most, or all of these sectors will be severely degraded or destroyed with limited resources to make repairs and replacements to these sector's systems. To that end, while all 16 critical infrastructure sectors are important, some sectors must be a priority for repair and restoration for the following reasons:

- Certain sectors are more interconnected than others and have dependencies that can cascade causing more immediate disruptions.
- Certain critical sector goods and services are more essential to support economic restoration than others.

To support development of the COTE response, CISA identified seven key critical infrastructure sectors for focus when reviewing plans and procedures. This determination was based on research, interagency and private sector stakeholder discussions, and survey responses, as well as advice from subject matter experts. The seven key critical infrastructure sectors are: Energy, Communications, Information Technology, Financial Services, Food/Agriculture, Transportation, and Water/Wastewater. These key sectors should be validated and updated via existing risk management forums and bodies after the further analysis that is called for in Recommendations 1.1 and 1.2.

These seven key critical infrastructure sectors are included in FEMA's Community Lifelines framework and their services are also detailed in CISA's NCF framework. The NCF framework indicates that the functionality of "Connect, Distribute, Manage, and Supply" are functions of government and the private sector so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The seven key sectors facilitate these NCFs. In addition, FEMA's Guide to Continuity of Government itself calls for the necessity of having critical resources available to conduct their operations plan, including fuel, power generation equipment, various communications methods, and technologies, including cell

phone service, and food and water. Finally, all of the Sector Specific Plans detail the criticality of these seven key critical infrastructure sectors.

RECOMMENDATION: All 16 critical infrastructure sectors are vital to our nation's economy and national security. While CISA reached a certain level of consensus on the seven sectors to initially prioritize based on our interviews and research of existing frameworks, departments and the SRMAs should further confirm and validate if these sectors are the correct prioritizations or if they should vary based on different significant event consequences.

3.6 Recommendations to Plan and Prepare for Economic Restoration After a Significant Event

CISA recommends the following considerations to advance the overall capability to plan and prepare for economic restoration. These recommendations can be addressed under existing federal government authorities, policies, plans, and frameworks. Table 3 below, details the recommendations.

3.6.1 Develop A Risk Based Approach Using Planning Scenarios

Creating a set of planning scenarios that would trigger the need to implement a response to a significant COTE type event will aid in the development of the aforementioned governance and gap analysis as well as ensure all sectors are prepared to respond to a significant event. These planning scenarios should incorporate data and insights from public and private stakeholders. Mapping these scenarios to mitigation strategies can assist in building resilience prior to an incident and support decisions on prioritization and reconstitution of the economy, post-event. Global economic risk, dependency analysis, and consequence modeling could identify scenarios that may cause national-level degradation to the NCFs and the seven key critical infrastructure sectors. While the focus and jurisdiction of COTE legislation is limited to the U.S., any economic recovery from a domestic significant event will involve the global economy. Understanding global economic risks, and options for risk mitigation, will strengthen any response to resuscitate the domestic economy. Information sharing among stakeholders is what ensures that the planning scenarios provide value. Developing trust among global partners will also be a key component.

RECOMMENDATION: As a part of their routine planning and analysis efforts, CISA recommends federal agencies create a set of economic-focused planning scenarios to aid both the development of the expanded gap analysis (Recommendation 1.1) and the response to a significant event. Utilizing data and insights from public and private stakeholders to establish a risk-based based approach using planning scenarios based on economic impacts would assist in building resilience prior to an incident and support decisions on prioritization and reconstitution of the economy post-event. These efforts can be adapted to continuity of the economy planning, global economic risk and dependency analysis, as well as consequence modeling and could identify scenarios that may cause national-level degradation to NCFs and the proposed seven key critical infrastructure sectors identified for initial analysis.

3.6.2 Define Data Needs to Support Economic Restoration

Currently, there are numerous federal data collection efforts and frameworks across the interagency. Oftentimes, federal data collection efforts are siloed and scattered across multiple agencies and may have strict limits on subsequent use or distribution, which inhibits the ability of U.S. government leaders to make timely policy and operational decisions, which will be needed during a significant event. Furthermore, agencies often rely on information provided by the private sector, which can sometimes be difficult to obtain.

RECOMMENDATION: CISA recommends that departments and agencies follow Recommendation 3.4.1 to better identify and define the data necessary for making economic restoration decisions and determine where there may be potential gaps in current data collection and analysis efforts. This information could be operationalized to support (1) information sharing among stakeholders, and (2) state

and local prioritization of critical infrastructure-related response and recovery activities. To develop emergency measures, assessments using the data can aid in anticipating potential cascading, escalating, and common cause failures to reach specific stakeholder's requirements. In addition, iterative and scalable dependencies and interdependencies governance can be integrated into existing risk and resilience assessment frameworks.

3.7 Analysis: Assessment of COTE Requirements A-S

CISA analyzed Requirements A-S primarily through the use of CISA's NCF frameworks, FEMA's NRF, Emergency Support Functions, Community Lifelines, PPD-8, PPD-21 and NCIPP, among others. In addition, the previous authorities and stakeholder analysis detailed in this response were central to this analysis. Requirements detailed here should be reviewed in conjunction with the gap and governance analysis, among the other recommendations. Agencies and sectors may want to consider utilizing the recommendations to enhance economic restoration issues as a part of their routine planning and analysis efforts.

Table 3: Requirements A-S

Requirement	Recommendations	Required Federal Stakeholders	Additional Required Stakeholders / Expertise	Representative Authorities/Analytical Frameworks	Data for Analysis
Requirement A: Distribution of Goods and Services	1. Articulate and maintain overarching framework that analyzes and categorizes which modes of distribution have most vulnerabilities and concentrated dependencies. 2. Create system models that map cascading consequences on other sectors and develop potential workaround solutions. 3. Initiate contingency planning. 4. Define key decision-making roles for prioritization of goods and services and coordination of seven key critical infrastructure sectors.	• DHS • USDA • DOC • DOE • DOT • EPA • FCC • Treasury	• Supply chain and logistics experts Relevant Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs)	• NCFs • PPD-8 • PPD-21 • EO 14017-America's Supply Chains	• Transportation dependencies • System models of the seven key critical infrastructure sectors to determine cascading impacts • Table-top exercises and stress testing lessons learned
Requirement B: Economic Functions of Relevant Actors	1. Expand ongoing risk analysis of critical infrastructure dependencies and interdependencies related to critical infrastructure to add economic functions and consequence analysis. 2. Identify and develop appropriate models. 3. Utilize Decision Consequence Analysis (DCA) approach to allow for a formalized decision-making process. 4. Regularly review and update interdependency data. 5. Assess potential supply chains workarounds and reserves that can help to alleviate the adverse impacts to key economic functions. 6. Augment sector prioritization analysis by conducting contingency and scenario planning.	• DHS • USDA • DOC • DOD • DOE • DOJ • DOT • EPA • FCC • FTC • HHS • Treasury	• Supply chain management, logistics and critical infrastructure experts • Relevant SCCs and GCCs	• Defense Production Act • NCFs • Relevant Sector Specific Plans	• Goods and services that have key dependencies to determine supply chain workarounds and necessity of potential reserves • Information regarding feasibility of Voluntary Agreements

Requirement	Recommendations	Required Federal Stakeholders	Additional Required Stakeholders / Expertise	Representative Authorities/Analytical Frameworks	Data for Analysis
	7. Explore feasibility of establishing Voluntary Agreements under Section 708 of the DPA.				
Requirement C: Critical Distribution Mechanisms	1. Assess, vet, and categorize prioritizations of various consequences surrounding a significant event, as priorities may change based on consequences.	• DHS • USDA • DOC • DOE • DOT • EPA • FCC • HHS • Treasury	• Supply chain and logistics experts • Relevant SCCs and GCCs	• NCFs • FEMA Community Lifelines • PPD-8 • PPD-21 • EO 14017- America's Supply Chains	• Transportation dependencies
Requirement D: Disruption of Economic Functions Causing Catastrophic Economic Loss Requirement E: Disruption of Economic Functions Undermining Response	1. Requirements D and E are extremely similar to Requirement B. All of these Requirements pertain to economic functions. As a result, the recommendations in response to Requirement D and E can be found in Requirement B. 2. Within the analytic framework of Requirement B, identify specific elements related to life safety.	• DHS • USDA • DOC • DOD • DOE • DOJ • DOT • EPA • FCC • HHS • Treasury	• Supply chain management, logistics and critical infrastructure experts • Relevant SCCs and GCCs	• Defense Production Act • NCFs • Relevant Sector Specific Plans	• Goods and services that have key dependencies to determine supply chain workarounds and necessity of potential reserves • Information regarding feasibility of Voluntary Agreements • Inventory of health functions relating to COTE emergencies
Requirement F: Federal Plans for the Continuity of Government (COG) and Continuity of Operations (COOP)	1. Consider consolidating or creating a central clearinghouse within federal government for critical infrastructure identification efforts led by federal government. 2. FEMA should continue to provide the private sector with the best practices that are developed and updated on an ongoing basis in federal continuity programs.	• DHS • USDA • DOC • DOD • DOE • DOJ • DOT • EPA • FCC • HHS	• COOP and COG, contingency and continuity planning experts and attorneys from seven key critical infrastructure sectors and interagency • Relevant SCC(s) and GCC(s)	• Federal Continuity Directive 1 & 2 • NCFs	• Develop criteria for appropriate consolidation of federal critical infrastructure efforts

Requirement	Recommendations	Required Federal Stakeholders	Additional Required Stakeholders / Expertise	Representative Authorities/Analytical Frameworks	Data for Analysis
		• Treasury			
Requirement G: Disruption of Industrial Control Networks	1. Align identification of critical industrial control systems (ICS) with the overarching infrastructure modeling proposed under Requirement B. 2. Continue to communicate with seven key critical infrastructure sectors about the frameworks and tools to increase resilience. 3. Undertake contingency planning to determine methods and timing of restoration of ICS. 4. Continue to monitor methods of attack on ICS systems. 5. Assess both the economic feasibility and practicality of analog and parallel systems to enhance ICS resilience and security.	• DHS • USDA • DOC • DOD • DOE • DOT • EPA • FCC • Treasury	• ICS experts • Network and cybersecurity experts • IT systems experts • Relevant SCC(s) and GCC(s)	• NIST Special Publication 800-82, Revision 2, "Guide to Industrial Control Systems (ICS) Security"	• Information regarding analog and parallel systems as well as other methods to increase ICS resilience • Threat monitoring • Key stakeholders
Requirement H: Preservation of Data	1. Articulate and maintain a framework to determine how government and private sector could restore or recreate data. 2. Verify that a critical records list is complete for all sectors. 3. Rank items in order of importance to protect most important items first, considering that some localities and organizations may have limited funds or skill sets. 4. Advocate for best practices for backing up and preserving critical data and how to incentivize government and industry action.	• DHS • USDA • DOC • DOE • DOJ • DOT • EPA • FCC • Treasury • SLTT	• All relevant SCC(s) and GCC(s) • Private sector continuity of operations experts • IT systems experts • Data recovery and forensic experts • Legal experts	• PPD-21 • Relevant SLTT and private sector legislation, agreements, frameworks, for preserving or storing personal and commercial data	• Information on feasibility and legality of preserving data • Best practices of data preservation, such as Sheltered Harbor • Framework and ranking for types of data to be stored or recreated • Stakeholder input

Requirement I: Lack of Raw Materials, Industrial Goods Undermining Recovery	1. Identify materials and goods that are originated, produced, manufactured, or assembled in adversarial nations or regions. Emphasis should also be on materials and goods that have few substitutions, long extraction or production lead times, or limited supply.	• DHS • USDA • DOC • DOD • DOE • DOT • EPA • FCC • Treasury	• Raw material and minerals supply chain experts • Manufacturing, production, and supply chain experts • Relevant SCC(s) and GCC(s)	• EO 14017 – America's Supply Chains • Energy Act of 2020	• Criticality classification system for at risk goods and services
Requirement J: Supply Chain Diversification	1. Identify key products and components that are difficult to substitute, have long lead times, come from a single source or single region/country, or are from adversarial nations. 2. Identify core elements of seven key critical infrastructure sector supply chains that could cause cascading adverse impacts on both individual and cross-sector supply chains. 3. Prepare supply chain workarounds in anticipation of significant event. 4. Ensure seven key critical infrastructure sectors employ best practices for supply chain resilience.	• DHS • USDA • DOC • DOD • DOE • DOT • EPA • FCC • Treasury	• Manufacturing, production, and supply chain experts • Logistics experts • Contingency planning experts • Relevant SCC(s) and GCC(s)	• EO 14017 – America's Supply Chains • Federal Acquisition Supply Chain Security Act of 2018	• Criticality classification system for at risk products and components • Cascading impacts of supply chain bottlenecks and chokepoints • Stakeholder input
Requirement K: Strategic Reserve	1. Consider feasibility and necessity of creating stockpiles, given that potential items in the reserve may need to continually shift. 2. Determine which items may be worthy of stockpiling and/or reserves, working with necessary industry and government experts to determine which items are critical to economic and national security. 3. Determine availability of goods in large quantities, costs, spoilage, and	• DHS • USDA • DOC • DOD • DOE • DOJ • DOT • EPA • FCC • HHS • Treasury	• Manufacturing, production, and supply chain experts • Strategic reserve experts • Economists • Chamber of Commerce • Relevant SCC(s) and GCC(s)	• 42 U.S. Code § 6234 - Strategic Petroleum Reserve • Section 161 of the Energy Policy and Conservation Act (EPCA) • Public Health Service Act • Defense Production Act	• Business case and national security analysis for expansion of strategic reserves • Stakeholder input • Market impacts due to strategic reserve expansion

	technological irrelevance that are areas of concerns. 4. Review detrimental impact that reserves and stockpiles can have on the free market and weigh that against economic and national security needs.			• Strategic and Critical Materials Stockpiling Act	
Requirement L: Swift Transport and Delivery of the Raw Materials and Industrial Goods	1. Explore implementation of national resource management programs that would support swift transport and delivery of stockpiled items to prioritized recipients during a significant event, in line with national priorities.	• DHS • USDA • DOC • DOD • DOE • DOT • EPA • FCC • Treasury	• Logistics experts • Program management experts • Security experts • Relevant SCC(s) and GCC(s)	• 42 U.S. Code § 6234 - Strategic Petroleum Reserve • Section 161 of the Energy Policy and Conservation Act • Public Health Service Act • Defense Production Act • Strategic and Critical Materials Stockpiling Act	• Framework for safe and secure delivery of goods and services in constrained environment
Requirement M: Prioritization for Distribution	1. Perform risk analysis of critical infrastructure dependencies and interdependencies related to critical economic functions and consequence analysis. 2. Partner with private sector stakeholders to establish broad principles which can be applied to analytic results and guide prioritization. 4. Create risk architecture composed of seven critical infrastructure sectors to establish the key assets, networks and systems that support sector operational processes. 5. Identify entities that are key providers of elements of each operational process and function.	• DHS • USDA • DOC • DOD • DOE • DOT • EPA • FCC • Treasury	• Risk management and supply chain experts • Prioritization experts • Strategic planners • Program management experts • Stakeholder engagement experts • SLTT stakeholders • Relevant SCC(s) and GCC(s)	• NCFs • Defense Production Act	• Key assets and networks and systems of the seven key critical infrastructure sectors and their associated processes, sub-processes, and dependencies

Requirement N: Extending credit or Providing Other Financial Support	1. Work with public and private sector economists and key private sector parties to determine types of stabilization, stimulus or incentive programs that are appropriate for the different consequence scenarios following a significant event. 2. Examine performance of recent federal stimulus programs and packages.	• Congress • DOC • Executive branch • Federal Reserve • Treasury • SBA	• U.S. based SIE Banks • U.S. Chamber of Commerce • Fortune 500 Business Roundtable • Economists	• Section 13(3) of the Federal Reserve Act	• Data regarding existing, commercial paper and credit facilities and municipal liquidity facilities; existing stimulus and incentive programs • Historical performance data
Requirement O: Prioritization of Categories of Employees	1. Review CISA's "Essential Critical Infrastructure Workforce" list in relation to seven key critical infrastructure sectors to determine if the list can be better scoped and based on potential consequences of various possible events. 2. Determine whether list(s) should be shared in advance with stakeholders to obtain their input. 3. Develop potential timelines of when list(s) should be released, following a significant event.	• Executive branch • DHS • USDA • DOC • DOD • DOE • DOT • EPA • FCC • Treasury	• Economists • Fortune 500 Business Roundtable • Relevant SCC(s) and GCC(s)	• Cybersecurity and Infrastructure Security Agency Act of 2018	• "Essential Critical Infrastructure Workforce" list and NAICS codes • Stakeholder input
Requirement P: Material and Operational Support to The Defense of The U.S.	1. Consider developing integrated approach to prepare for and mitigate potential resource conflicts between DOD and civilian government counterparts. 2. Determine if the Office of the Secretary of Defense and Defense Logistics Agency may be best postured to detail DOD's efforts for supply chain diversification and stockpiling requirements. 3. Identify what civilian federal departments and agencies need to become more self-sufficient during significant events. 4. Ensure that civilian federal interagency continues to support	• DHS • USDA • DOC • DOD • DOE • DOT • EPA • FCC • Treasury	• Resource management experts • Contingency planning experts • Defense readiness and preparedness experts • Defense logistics experts • Supply chain experts • Relevant SCC(s) and GCC(s)	• Defense Production Act • Title VI Robert T. Stafford Disaster Relief and Emergency Assistance Act	• Prioritization of defense and civilian needs of goods and services

	DOD efforts to understand what civilian critical infrastructure and services are necessary to maintain the Defense Industrial Base and to support DOD missions, including force projection.				
Requirement Q: Authority for DHS, National Guard, DOD to Assist in a Recovery	1. Ensure existing frameworks adequately account for the authorities required for the supervision, coordination, direction, and execution of continuity of the economy requirements.	• DHS • USDA • DOC • DOD • DOE • DOT • EPA • FCC • Treasury	• SLTT stakeholders • Law, regulation, policy analysis, governance	• Title 10, Title 32, Title 50 Defense Production Act • Robert T. Stafford Disaster Relief and Emergency Assistance Act	• National defense and emergency management to identify defense capabilities to be used for non-military purposes • State constitutions and laws for National Guard in state status • Defense resource authorities
Requirement R: Authority and Capability of Heads of Other Agencies	1. Ensure that the authorities for supervision, coordination, and direction, and the operational authorities to carry out economic recovery responses are accounted for in existing frameworks. 2. Conduct comprehensive review of government resource authorities and responsibilities. 3. Identify and, where necessary, develop or expand capabilities to execute the elements of DPA appropriate to mitigate the impacts of significant events.	• All federal D/A	• Law, regulation, policy analysis, governance, resource management, emergency response experts	• EO 12656 • National Preparedness System including 6 U.S.C. 753 • PPD-8 • Robert T. Stafford Disaster Relief and Emergency Assistance Act • Federal Power Act • Public Health Service Act • Defense Production Act	• Government authorities and responsibilities related to preparedness and response, including the Defense Production Act • Cross-sector framework that details authorities for supervision, coordination, and operations • NIMS and other common sets of terms for events requiring Whole-of-Government response
Requirement S: Other Matters to Aid Resilience of the Economy	1. Undertake stakeholder engagement and enrollment process for the wide range of public and private partners regarding the importance of continuity of economy efforts. Need to provide some level	• DHS • USDA • DOC • DOD • DOE	• SLTT stakeholders • Stakeholder engagement experts • Change management consultants	• N/A	• Stakeholder analysis, current/future state description, case for change, and expected barriers

	of commitment to assist in these efforts.	• DOT • EPA • FCC • Treasury	• Strategic communications experts • Relevant SCC(s) and GCC(s)		• Identified key stakeholders