Cyber Response and Recovery Act Program 180 Day Report

Fiscal Year 2022 Report to Congress
August 18, 2023

Homeland Security

Cybersecurity and Infrastructure Security Agency

Message from the Director

August 18, 2023

I am pleased to present the following, "Cyber Response and Recovery Act Program 180 Day Report," prepared by the Cybersecurity and Infrastructure Security Agency (CISA).

This report has been compiled pursuant to a requirement in the Joint Explanatory Statement that accompanies the Fiscal Year (FY) 2022 Department of Homeland Security (DHS) Appropriations Act (P.L. 117-103). This report provides an overview of CISA's program implementation strategy and the reasons this strategy is adopted. The report also provides information on how the Cyber Response and Recovery Fund (CRRF) would be leveraged in response to a significant incident.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable David Joyce
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Henry Cuellar
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Chris Murphy
Chair, Senate Appropriations Subcommittee on Homeland Security

The Honorable Katie Britt
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to CISA Legislative Affairs at (202) 819-2612.

Sincerely,

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

This report provides an overview of CISA's implementation plan for the Cyber Response and Recovery Act, allowing for the capabilities and authorities provided to CISA to be leveraged during a significant incident. The report also fulfills the requirement included in the Joint Explanatory Statement accompanying the FY 2022 DHS Appropriations Act (P.L. 117-103), providing information on how the CRRF would be leveraged in response to a significant incident.

Cyber Response and Recovery Act 180 Day Program Report

Table of Contents

I. Legislative Language

The Joint Explanatory Statement accompanying the Fiscal Year 2022 Department of Homeland Security Appropriations Act (P.L. 117-103) includes the following requirement:

> *Cyber Response and Recovery Fund (CRRF).*—The Infrastructure Investment and Jobs Act, 2021 (IIJA), (Public Law 117-58) appropriated $100,000,000 for the CRRF, of which $20,000,000 is available for fiscal year 2022, the same as the amount requested in the President's fiscal year 2022 budget request. Accordingly, the agreement does not provide additional funding to CRRF. Further, the briefing required in House Report 117-87 has already been provided and is therefore no longer required. The agreement directs CISA to provide a plan for the CRRF within 180 days of the date of enactment of this Act. The plan shall include: how CISA will determine—using clear metrics—when CRRF support will be provided by taking into consideration private sector post-incident resources, and if such support will be reimbursable, non-reimbursable, cost-sharing, or provided as a grant; what steps recipients of CRRF support are required to take for known prevention measures to qualify; what incentives, if any, will be provided to encourage recipients to take such steps; and CISA's ability to quantitatively identify a private sector recipient's ability to repay such assistance before offering such support. Further, the plan shall include a projection of future years' costs and a discussion of the categorization of any future funding for the Fund (e.g., defense, non-defense, disaster, emergency).

II. Background

The Homeland Security Act of 2002, as amended by the Cyber Response and Recovery Act (CRRA), authorizes the Secretary of Homeland Security, in consultation with the National Cyber Director, to declare a significant incident for the purpose of enabling activities described in the CRRA. The Secretary, in consultation with the National Cyber Director, can issue a declaration upon a determination that (A) a specific significant incident has occurred or is likely to occur imminently, and (B) otherwise available resources, other than the Cyber Response and Recovery Fund (CRRF), are likely insufficient to respond effectively to or mitigate the specific significant incident identified.

Once a declaration has been issued, Section 2234 of the Homeland Security Act provides that the CRRF is available for use by the Cybersecurity and Infrastructure Security Agency (CISA) for:

- Coordinating the asset response activities of federal agencies in response to a declared specific incident; coordinating with appropriate entities, which may include public and private entities and state and local governments with respect to their asset response activities, as well as coordinating with law enforcement agencies with respect to their investigations and threat response activities, and emergency management and response agencies;
- Response and recovery support, for the specific declared significant incident, "to federal, state, local, and tribal, entities and public and private entities"[1] (on a reimbursable or non-reimbursable basis), including through asset response activities and technical assistance (such as vulnerability assessments and mitigation, technical incident mitigation, malware analysis, analytic support, threat detection and hunting, and network protection);
- As the CISA Director determines appropriate, grants for or cooperative agreements with, federal, state, local, and tribal public and private entities to respond to, and recover from, the specific significant incident associated with a declaration (such as hardware or software to replace, update, improve, harden, or enhance the functionality of existing hardware, software, or systems); and,
- Advance actions to arrange or procure additional resources for asset response activities or technical assistance the Secretary determines necessary (such as entering into standby contracts with private entities for cybersecurity services or incident responders in the event of a declaration).

[1] CRRA § 2234(a)(2): https://www.congress.gov/117/bills/s1316/BILLS-117s1316rs.pdf

III. Implementation Plan

In implementing the CRRA consistent with CISA's regular responsibilities and authorities under statute and executive branch policy—a whole-of-government response to responding to significant cyber incidents—CISA has worked to facilitate the rapid expansion of operational capabilities to support a significant incident declaration and leverage of the statutorily authorized uses of the CRRF in the event of declaration. To achieve this goal, CISA first focused on enabling authorized uses of the CRRF that align with well-established existing capabilities and programs within CISA, namely, the asset response coordination and response and recovery support authorized uses in § 2234(a)(1) and (2), respectively. This will be followed by efforts to enable other authorized uses of the CRRF that provide new authorities to CISA and require the development of novel policies, procedures, and capabilities, namely, the grant and cooperative agreement authorized use in § 2234(a)(3).

As a result, CISA intends to implement the CRRA in phases. In the initial phase, CISA has defined the required internal capabilities and processes to execute a significant incident declaration process, should it be immediate and necessary, and to use the CRRF in the event of a declaration to supplement existing asset response coordination and response and recovery capabilities. In future implementation phases, CISA will build the capabilities and processes required to enable use of the CRRF for grants and cooperative agreements with federal, state, local, and tribal public and private entities. As CISA continues to develop its processes and capabilities, CISA will work with appropriate Federal partners to integrate them into the broader whole-of-government response to significant cyber incidents.

A. Initial Uses of CRRF Funding for Significant Incidents

Declaration Process:

CISA has designed an internal process to collect the relevant information and documentation to facilitate the Secretary's declaration of a significant incident, in consultation with the National Cyber Director, and in compliance with § 2233(a)(1) of the Homeland Security Act. Specifically, this process plans to use the CRRA as a complement to existing CISA and whole-of-government response to significant cyber incidents and incorporate appropriate staff-level coordination within CISA and the Office of the National Cyber Director to ensure that the Secretary has the necessary information to determine whether the two required conditions for a declaration in § 2233(a)(1) have been met.

First, it must be determined that a specific significant incident has occurred or is likely to occur imminently. To identify incidents for possible consideration as a significant incident, CISA will leverage existing executive branch processes, policies, and bodies for identifying and coordinating responses to significant cyber incidents, developed pursuant to Presidential Policy Directive 41. CISA will also leverage the National Cyber Incident Scoring System (NCISS)[2], a repeatable and consistent mechanism currently used by CISA, in coordination with the Sector

[2] https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss

Risk Management Agencies and other appropriate Federal partners, for scoring cyber incidents based on estimated risk and severity. If CISA determines that a significant incident declaration may be warranted, CISA will compile relevant information known about the incident through CISA's direct activities and through appropriate interagency staff-level coordination for consideration by the Secretary.

Second, it must be determined that "otherwise available resources, other than the Fund, are likely insufficient to respond effectively to, or to mitigate effectively, the specific [identified] significant incident." CISA will evaluate its available resources through comparison of planned versus unplanned resource requirements or through the evaluation of short-term capability (or capacity) requirements that emerge or are expected to emerge directly because of the nature of the specific significant incident e.g., requirements that fall outside the scope of "normal" operations, which require supplemental funding from the CRRF to respond effectively. If CISA determines that a significant incident declaration may be warranted, CISA will compile relevant information known about the identified likely resource insufficiency for consideration by the Secretary. CISA will ensure appropriate consultation with the Office of the National Cyber Director, and coordination with other appropriate administration and interagency entities prior to the Secretary declaring a significant incident.

CRRF Initial Planned Uses

During the initial phase of CRRA implementation, in the event of a significant incident declaration, CISA plans to use the CRRF for the first two authorized uses in § 2234(a)(1) and (2) of the Homeland Security Act – asset response coordination and response and recovery support, respectively. As described more fully below, these two authorized uses align with CISA's existing capabilities, structure, and contract vehicles, allowing for effective use of any available funds from the CRRF in an expeditious manner.

- **Asset Response Coordination:** As the designated lead federal agency for asset response activities in the event of a significant cyber incident, CISA maintains established asset response coordination capabilities. These capabilities, which focus on coordinating public and private sector asset response activities to provide unity of effort, enable CISA to coordinate with any entities affected by, or otherwise providing support in response to, the incident, and are reinforced with the CRRA. CISA's Cybersecurity Division (CSD), led this effort during the 2020 SolarWinds supply chain compromise and the recent Log4J vulnerability response by conducting outreach to impacted and likely impacted entities, coordinating requests for technical assistance from the Federal Government where appropriate, and developing and publishing technical response and recovery guidance. Per § 2234(a)(1) of the Homeland Security Act, CISA can use the CRRF during a declared significant incident to support these activities, enabling CISA to coordinate with additional impacted entities and at a greater level. In the event of a significant incident declaration, CISA would utilize the CRRF to surge personnel, including program support, subject matter experts, and existing staff, based on the identified resource needs of the specific incident, to enable CISA to more effectively conduct asset response coordination activities with a broader array of impacted entities during declared significant incidents.

- **Response and Recovery Support:** CISA's CSD leads the Agency's effort to provide response and mitigation support to impacted entities. CSD achieves this mission through information-sharing and by providing non-reimbursable voluntary technical assistance in the form of incident response support, mitigation recommendations, malware analysis, analytic support, and threat detection and hunting engagements to public and private sector entities. These current offerings are already provided by CISA on a non-reimbursable basis and constitute technical assistance rather than direct federal assistance or federal assistance in the form of financial assistance. For these types of services already within CISA's mission, CISA does not currently envision requiring recipients of this technical assistance to reimburse or contribute a non-federal share toward the cost of the services. In addition, as these services are currently provided on a non-reimbursable basis, the ability for a recipient to repay such assistance is not specifically evaluated. Further, while CISA routinely strives to encourage non-Federal entities to adopt heightened cyber hygiene through voluntary guidance and the offering of no-cost cybersecurity services, CISA does not currently use the taking of proactive cybersecurity steps as a condition or requirement for accessing CISA support in the event of an incident, nor does it plan to in the event of a significant incident. CSD's support offerings have pre-existing application and service prioritization processes, which includes considerations such as the functional impact, observed activity, threat actor characterization, recoverability (including an entity's ability to effectively recover without external support), and cross-sector dependencies of the incident or group of related incidents reported. In the event of a significant incident declaration, CISA would use the CRRF to provide support to impacted entities responding to, and recovering from, the specific significant incident, which could include, among other types of assistance, technical incident mitigation support to help entities restore impacted infrastructure and implement proper network protections.

B. Future Use of CRRF Funding on Significant Incidents

Building on the foundation established in Phase One, Phase Two of CISA's CRRA Implementation Plan focuses on the grant and cooperative agreement authorized uses for the CRRF detailed in § 2234(a)(3) of the Homeland Security Act. CISA's use of these authorities require new internal policies, processes, and capabilities, as CISA is required to comply with 2 C.F.R. Part 200, the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for federal awards to non-federal entities. Included among these regulatory requirements is the publication of a Notice of Funding Opportunity (NOFO), reviewing the merit of applications submitted in response to a NOFO, and issuing a federal award notice including specific information. CISA is currently evaluating the most optimal program structure necessary to create the grant and cooperative agreement program authorized in the CRRA, leveraging expertise from partner agencies such as the Federal Emergency Management Agency. CISA will consider the inclusion of metrics for when CRRF support will be provided, taking the following into consideration:

- Private sector post-incident resources;
- Whether direct federal assistance or financial assistance provided will require a cost-share; and,

- What steps recipients of direct federal or financial assistance are required to take for known prevention measures to qualify.

IV. CRRF Future Years' Projections

Due to the inherent uncertainty regarding frequency or severity of significant incidents, CISA is planning for future years' funding projections based upon multiple significant incident scenarios, identifying operational requirements to effectively respond to or mitigate these potential significant incidents (where otherwise available funds likely are insufficient to respond effectively), and exploring how to most effectively use the CRRF in the event of a declaration to satisfy these operational requirements. As warranted, requests for additional funding for the CRRF will be included in future years' Presidential Budget proposals.

V. Conclusion

The Homeland Security Act of 2002, as amended by the CRRA, authorizes the Secretary, in consultation with the National Cyber Director, to declare a significant incident, directs and authorizes CISA's actions, and makes available for use the CRRA-established CRRF for authorized purposes. CISA is leading the development of the tools, capabilities, and managerial structure to ensure the authorities and capabilities are utilized effectively, efficiently, and responsibly to manage resources and to achieve the best outcome of the safety and security of the United States.

The CRRA will increase CISA's flexibility in responding to, and supporting the recovery from, declared significant incidents and otherwise address the impacts of a declared significant incident. It will further our efforts to work effectively with public and private sector impacted entities responding to, and recovering from, incidents likely to result in demonstrable harm to the people, economy, foreign relations, and national security of the United States.

As this capability is developed and matured, CISA will continue to consult with appropriate interagency partners to integrate the CRRA processes into the broader whole-of-government response to significant cyber incidents.

VI. Appendix

Abbreviation	Definition
C.F.R.	Code of Federal Regulations
CISA	Cybersecurity and Infrastructure Security Agency
CRRA	Cyber Response and Recovery Act
CRRF	Cyber Response and Recovery Fund
CSD	Cybersecurity Division
DHS	Department of Homeland Security
FY	Fiscal Year
NCISS	National Cyber Incident Scoring System
NOFO	Notice of Funding Opportunity
P.L.	Public Law