



# National Risk Management Center Operating Model

*April 19, 2023*

Fiscal Year 2022 Report to Congress



**Homeland  
Security**

*Cybersecurity and Infrastructure Security  
Agency*

# Message from the Director

April 19, 2023

The following report, “National Risk Management Center Operating Model,” has been prepared by the Cybersecurity and Infrastructure Security Agency (CISA).

This document has been compiled pursuant to a requirement in House Report 117-87, which accompanies the Fiscal Year 2022 Department of Homeland Security Appropriations Act (P.L. 117-103).

This report outlines the process by which CISA’s National Risk Management Center (NRMC) will manage, transfer, and resource priority cross-divisional risk initiatives.

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

The Honorable Dave 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

The following report identifies new analytic priorities and is a strategy for transitioning NRMC analytic models that are operational in nature to other CISA divisions.

The strategy includes the development of criteria for risk initiative “go/no-go” decisions and decision criteria for initiative lifecycle options. The “go/no-go” criteria allow NRMC to decide more easily whether to move forward with an initiative decision based on:

- How high a priority it is on the NRMC Risk Register;
- If the NRMC is resourced adequately to handle the initiative/product;
- If the initiative/product requires engagement beyond an individual sector, or if the scale of the issue exceeds available capability within the particular sector;
- If leadership has asked the NRMC specifically to tackle the risk; and/or
- If the NRMC brings a differentiated value to the risk.

The decision criteria for initiative lifecycle options selected at the outset of NRMC’s involvement allow NRMC to determine the level of involvement and resources from the start. The lifecycle options are as follows:

- **Sustain:** An initiative will be sustained when it requires extended programmatic support capabilities from NRMC to mitigate the corresponding risk prioritized on the NRMC Risk Register.
- **Sunset:** An initiative will sunset with no further action when sufficient progress is made without the need for the ongoing sustainment of an operationalized risk management effort.
- **Transition:** The NRMC Assistant Director may recommend to CISA leadership that another CISA division or program is positioned better to lead risk mitigation activities in the longer term. It is not the intention of the NRMC to transition staff or other funded resources.

There will be no budgetary impact for this decision and NRMC aims for a funding-neutral approach to this process, keeping all staff and budget within the larger program areas while individual program resources may transition.

NRMC’s strategy for identifying analytic priorities to create solutions for national risk management efforts is integral to DHS’s goals for securing cyberspace and critical infrastructure. This collaborative multi-disciplinary approach eliminates silos to put forward the best resources, to improve understanding of threats to critical infrastructure, to buy down risk, and to build our Nation’s resilience.



# National Risk Management Center Operating Model

## Table of Contents

I.	Legislative Language.....	1
II.	Background.....	2
III.	NRMC Initiative Operating Model.....	3
IV.	Conclusion.....	6
V.	Appendix: Abbreviations.....	7

# I. Legislative Language

This report was compiled in response to direction in House Report 117-87, which accompanies the Fiscal Year 2022 Department of Homeland Security Appropriations Act (P.L. 117-103).

House Report 117-87 states:

*National Risk Management Center (NRMC).*—The NRMC has the potential to provide critical analysis of cross sector risks and interdependencies to inform more strategic security investments by both the public and the private sectors. When the NRMC was established in 2018, its work was driven by a targeted series of “sprints,” many of which are ongoing. Some, such as the Pipeline Security Initiative and the Election Security Initiative, have derivatives which are operational in nature, but unfortunately have not been transitioned to an operational division within CISA. The Committee is also concerned that the retention of operational programs at the NRMC is blurring its mission and stifling its ability to take on new analytic projects. CISA is therefore directed to submit an NRMC strategy, not later than 180 days after the date of enactment of this Act, for transitioning analytic models with operational uses to other CISA divisions and for identifying new analytic priorities. The strategy shall include any budget considerations affecting the transition of these capabilities out of the NRMC.

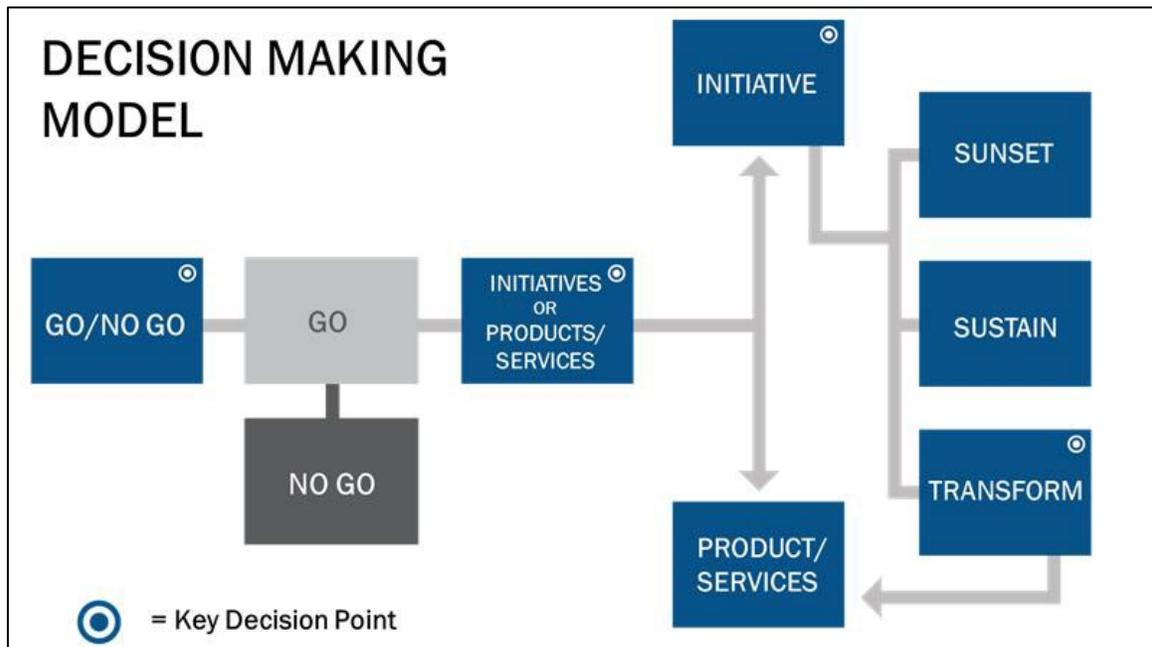
## II. Background

This report describes three lifecycle options for cross-divisional risk initiatives within the NRMC, discusses the broader Cybersecurity and Infrastructure Security Agency (CISA) implications of enacting the initiative lifecycle options, and provides a high-level overview of short-term implementation steps.

CISA is responsible for leading strategic risk-reduction efforts in a rapidly changing threat environment to enhance the Nation's resilience. The NRMC leverages its core capabilities to support this mission, collaborating with partners to analyze and reduce risks to our Nation's critical infrastructure using the National Critical Functions (NCF) Risk Management Framework. To operationalize this risk management mission, the NRMC assumes risk initiatives that are staffed initially by risk and technical experts where the topics of analysis vary depending on the risk environment or leadership priorities without adjustment to the funding for the organization.

Risk initiatives within the NRMC typically address risks that are novel or cross-divisional in nature. In some cases, risk initiatives remained within the NRMC as long-term efforts. According to CISA leadership guidance, priority risk initiatives are not intended to be permanent programs managed by the NRMC but either will transition to other parts of CISA or will sunset as risks are deemed adequately recognized and are being addressed.

### III. NRMCM Initiative Operating Model



#### *Initiative/Product Lifecycle Process*

Potential risk initiatives/products addressed by the NRMCM originate from a variety of sources including the NRMCM Risk Register, leadership direction, and critical infrastructure as supported by the NCF Framework.

NRMCM makes the “go” decision based on the NRMCM Assistant Director’s evaluation of the following factors:

- it is a high priority on the NRMCM Risk Register;
- the NRMCM is resourced adequately to tackle the initiative/product;
- the initiative/product covers multiple NCFs;
- leadership has asked the NRMCM specifically to tackle the risk; and
- the NRMCM brings a differentiated value to the risk.

NRMCM makes the “no-go” decision based on the NRMCM Assistant Director’s evaluation of the following factors:

- the initiative/product is not a high priority on the NRMCM Risk Register;
- the NRMCM is not resourced correctly to respond to the initiative/product;
- it only affects a single NCF; and
- the NRMCM does not bring a differentiated value to the initiative/product.

With a “go” decision, the NRMC Assistant Director also will determine whether an initiative lifecycle option will become an initiative or a product. The options and criteria for each are laid out below:

- **Products or Services Option:** Describes a condition where a risk owner accepts an identified risk/initiative product but has a limited set of resources and requires the NRMC’s specialized technical assistance to operationalize risk management. When the product or service has matured enough to be self-sufficient or the owner sustainably can buy down the risk, it will move to close out the risk/initiative.
- **Initiative Option:** Describes a condition where no risk owner is identified, accepting, or resourced, and NRMC is unable to pursue the products and service option. In addition, the risk requires NRMC’s differentiated value, is novel or covers multiple NCFs, or leadership has directed NRMC to operationalize risk management within the NRMC. For each initiative, NRMC assesses the operational environment as well as other internal and external NRMC drivers to determine the disposition method of a time-limited risk-management initiative.

When NRMC leadership determines that a product, service, or an initiative should continue, NRMC will work within CISA to identify the appropriate division or program to accept the responsibilities. Whether continuing operations within the NRMC, exemplified by Election Security, or transferring the responsibility to another entity, NRMC will ensure that the gaining organization has had time to validate authorities and program requirements for potential future resourcing requests.

At any time during this process, NRMC leadership may recommend to CISA leadership to move an initiative to the closeout or transition phases. Options for sustainment, sunseting, and transition are described in detail below and include cessation of work or transitioning the program to a longer term effort with dedicated resources.

## **Initiative Lifecycle Options: Criteria, Transformation, and Governance**

### ***Decision Criteria***

Determining at the outset which lifecycle option best aligns to the initiative allows for NRMC to plan its level of involvement and desired end state appropriately. Without this decision, NRMC’s success may be affected by inadequate resourcing, project delays, and potential barriers to transitioning or sunseting initiatives successfully. The NRMC Assistant Director is responsible for recommending an initiative lifecycle option.

1. **Sustain:** NRMC will sustain an initiative when it requires extended programmatic support and capabilities from NRMC, to mitigate the corresponding risk prioritized on the NRMC Risk Register. NRMC must: 1) be resourced and capable of sustaining the program, or 2) work with CISA leadership to request adequate resources.
2. **Sunset:** NRMC will sunset an initiative with no further action when sufficient progress is made without the need for the ongoing sustainment of an operationalized risk

management effort. The issue will be monitored on the NRMC Risk Register, but it will not be an NRMC or CISA priority for action.

- 3. Transition:** NRMC will recommend transitioning an initiative when it identifies another CISA division or program that is positioned better to lead risk mitigation activities in the longer term. NRMC leadership may recommend the transfer of specific activities, lines of effort, and products to that organization when it is resourced to, capable of, and authorized to assume ownership. No NRMC budget, staff, or materials will leave NRMC when the initiative is transitioned. Once the requirement is transitioned successfully, NRMC resources are reallocated to address risk as identified in the NRMC Risk Register.

The NCF Risk Register offers a successful example of product transition. Use of the NCF Risk Register is consistent and does not transform over time. However, NRMC uses the NRMC Risk Register as a sustained item within operations and transfers knowledge and prioritization insights across the organization to promote informed decision-making.

NRMC will monitor its initial decision criteria to assess how an initiative should be implemented. NRMC will revisit the criteria throughout implementation to determine if the final disposition needs to be adapted and transformed. The lifecycle option then will be implemented in the closeout phase.

An initiative may transform from one lifecycle option (sustain, sunset, or transition) to another when the risk landscape shifts. Some initiatives may shift to a new lifecycle option, while others may remain. Similarly, NRMC may develop new lines of effort in response to evolving risk criteria.

## **Resourcing**

As referenced at various points throughout this report, this is a budget-neutral process. Large programs rarely transition, and the process typically will involve transferring small products and services, so there is virtually no budget impact. NRMC will keep the staff and budget within larger program areas. In unusual situations, with a change in budget or authority shift, NRMC leadership may recommend that a program be moved. Any associated transfer of resources would be executed in accordance with statutory requirements and only after the successful completion of applicable agency, Department, and Administration resource planning processes.

## IV. Conclusion

This NRMC Operating Model outlines the process for initiative management at NRMC. Collaboration at all levels of government is essential to ensure that areas of shared risk are addressed and managed in a way that enhances our national security. This collaboration allows NRMC to increase its effectiveness, as well as increases the safety to cyberspace and critical infrastructure sectors.

Overall, NRMC will take a funding-neutral approach to this process, keeping all staff and budget within the NRMC program area, while initiatives or products may transition. Rather than transferring budget and staff as it initiates and transitions various risk initiatives, NRMC instead will seek to transfer the knowledge and support necessary to ensure that receiving entities have the appropriate information and products to support prioritization of risk-management activities and to inform risk-based decision-making.

## V. Appendix: Abbreviations

<b>Abbreviation</b>	<b>Definition</b>
CISA	Cybersecurity and Infrastructure Security Agency
NCF	National Critical Function
NRMC	National Risk Management Center