CROSS-IMPACTS FACILITATOR GUIDE

Secure Tomorrow Series

***Non-federal facilitators**: The Cybersecurity and Infrastructure Security Agency (CISA) has provided this toolkit as a starting point for your organization to address these critical issues. Please feel free to expand upon or adapt these exercises and tools to your needs. In several places throughout the document, we have provided guidance for federal facilitators regarding participants, process, and information protections. This guidance is based upon federal requirements, which may differ from state and local considerations. Please consult with your organization to consider what language or actions you will need to take in hosting a session.*

GOAL

This activity allows participants to explore, in a structured way, emerging and evolving risks and risk mitigation strategies pertaining to the topics of data storage and transmission, anonymity and privacy, and trust and social cohesion. Participants will focus their attention on six intersections of (1) key drivers of change, and (2) specific National Critical Functions (NCFs).[1]

Participants will come away with a better understanding of the ramifications of these drivers of change for different NCFs.

KEY OUTPUTS

- A list of plausible risks, organized around NCFs, pertaining to: (1) data storage and transmission; (2) anonymity and privacy; or (3) trust and social cohesion
- A corresponding set of risk mitigation strategies that would increase security and resilience of critical infrastructure and critical systems supporting these NCFs

RECOMMENDED PARTICIPANTS

*[**Please note:** This activity requires between 8 and 12 participants. Invitations to participate should focus on individuals at the mid- to senior career level who are interested in exploring longer-term risks to critical infrastructure (CI) to enable effective risk management. To provoke new lines of thinking about risks to CI and systems (either directly or through cascading impacts), we recommend that you seek broad representation from regional Cybersecurity and Infrastructure Security Agency (CISA) personnel; state, local, tribal, and territorial planners; fusion center and intelligence community representatives; and other private-sector, non-profit, think-tank, and academic stakeholders. In particular, individuals with interest and expertise in privacy and anonymity, data storage and transmission, and trust and social cohesion, and individuals who are already familiar*

[1] National Critical Functions (NCFs) are those 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.

with strategic foresight, are encouraged to participate. Please review the read ahead for your topic of interest to better understand the associated drivers of change and NCFs that the session will potentially cover and use this knowledge to target participants.]

[Once known, this section of the guide would list the participants, their titles, and the agencies/organizations they represent.]

FORMAT

This activity is designed for a period of four hours. The remainder of this facilitation guide is built around a virtual execution of the activity.[2]

SUPPORT STAFF

- Facilitator
- Documentation lead

SUPPORT MATERIALS

- Read-aheads for each of the cross-impacts session topics are available
- Virtual meeting platform
- Web-based platform that provides a virtual whiteboard (to construct the matrix of drivers of change and NCFs) and allows for real-time voting of intersection points

PREPARATION

The facilitator should become familiar with the specific topic (of the three) that is being explored. Research materials for all three topics are available upon request from SecureTomorrowSeries@cisa.dhs.gov. The facilitator should also review the facilitation questions included in this guide.

Participants should receive the topic read ahead one week before the session. The facilitator should review the list of participants and familiarize themselves with the background and affiliation of each participant.

For virtual executions, the facilitator should be comfortable using the virtual platforms involved. Matrix displays (see the appendices) should be generated ahead of time and the associated website link to access the display should be included with each participant's invitation.

[2] Please note: This activity can easily be converted for an in-person event. Participants would simply conduct the activities outlined in this guide on a white board or large wall, using sticky notes to display their ideas. For more details, please contact SecureTomorrowSeries@cisa.dhs.gov.

AGENDA (SAMPLE)

1:00–1:15pm	Introductory remarks (welcome, participant introductions, objectives, and agenda)
1:15-1:30pm	Choose intersection points for discussion
1:30–3:00pm	Discuss intersection points 1 – 3 (emerging risks, evolving risks, and risk mitigation strategies)
3:00–3:15pm	Break
3:15–4:45pm	Discuss intersection points 4 – 6 (emerging risks, evolving risks, and risk mitigation strategies)
4:45–5:00pm	Final thoughts and wrap up
1:00–1:15pm	Introductory remarks (welcome, participant introductions, objectives, and agenda)

GENERAL INSTRUCTIONS

- **Foster and maintain a collaborative, respectful atmosphere.** Encourage different observations, opinions, and perspectives. The discussions will explore a variety of policies, actions, and issues, and participants will likely display different degrees of expertise on a particular discussion topic. These discussions are a no-fault, not-for-attribution exercise that focuses on the identification, analysis, and generation of possible threats, uncertainties, and risk management strategies for upcoming issues of concern.
- **Encourage participants to speak from their perspective.** Particular stakeholder groups may have prominent strategic needs. We can use a participant's unique perspective as a starting point for broadening the discussion to how it might apply to other stakeholder groups. If a participant is speaking from the perspective of a particular stakeholder group, remember to ask other stakeholder groups how this might also apply to their group.
- **Focus on CI security and resilience**. Focus participants on linking whatever needs/issues are being discussed to a risk for CI security and resilience. They can be indirectly connected and can certainly prompt a discussion about any complexities and tradeoffs involved, but we always want to come back to CI security and resilience. In other words, as the group is identifying emerging or evolving threats, ALSO have them elaborate on the nexus to CI, if it is not obvious.

ACTIVITIY SESSIONS

I. **INTRODUCTORY REMARKS** (1:00–1:15pm): After welcoming participants and facilitating participant introductions, the facilitator will introduce the topic and objectives, as well as outline the agenda.

Breakdown	1. Welcome 2. Participant introductions 3. Review of objectives, topic of interest, and desired outputs 4. Agenda
Facilitator Talking Points	▪ Suggest that participants keep their videos on to make it easier to engage and have more free-flowing discussions. ▪ Determine ahead of time with the session sponsor whether participants will receive a copy of the notes from the session. If so, inform participants so they can focus on the discussion (versus taking notes). ▪ Provide background information on the specific topic of interest (see appendixes for topic descriptions).

II. **CHOOSING INTERSECTION POINTS** (1:15–1:30pm): The facilitator will display the topic matrix for the topic of discussion (Appendix A, B, or C) and give a brief tutorial on how to use the virtual platform to vote on priority intersection points in the matrix, which will serve as the main discussion points for the session. It is recommended that this take the form of virtual "dot" voting, assigning a set of five dots of the same color to each participant, which are used to indicate preferred intersection points on the virtual whiteboard. Participants will have three minutes to vote for the five intersection points they would like to discuss. The facilitator should work with the session sponsor ahead of time to determine the criterion for voting. Suggested options for the criterion include:

- Intersection points with the greatest impact
- Intersection points that are the least understood
- Intersection points that represent areas of which participants have the most knowledge

The facilitator will then review the virtual whiteboard and choose the six most popular intersection points for discussion in the next session.[3] Given the potential for overlapping concerns across multiple NCFs and/or drivers of change, the facilitator should use his or her discretion to determine whether to combine two or more intersection points to discuss at the same time.

[3] Alternatively, if the sponsor desires, the facilitator can arrange the selection process such that each selected intersection point addresses a different driver of change. To accomplish this, the facilitator may need to constrain each participant to vote for no more than one intersection point in each row of the matrix.

Breakdown	1. Define drivers of change and NCFs. 2. Relay instructions for choosing intersection points. 3. Review matrix with participants' selections. 4. Choose six intersection points for further discussion.
Facilitator Talking Points	▪ The facilitator should be prepared to help participants come to a common understanding of each of the drivers and NCFs listed in the matrix rows and columns. ▪ The facilitator should have some latitude in steering the group's selection of the six intersection points for discussion (e.g., helping break ties, encouraging broad coverage of multiple NCFs or drivers of change).

III. **DISCUSSION OF EMERGING AND EVOLVING RISKS AND MITIGATION STRATEGIES** (1:30–4:45pm, with a 15-minute break at 3:00pm): The facilitator will facilitate a group discussion around each of the six chosen intersection points focused on emerging risks, evolving risks, and risk mitigation strategies.

Breakdown	For each intersection point, facilitate discussion to expound upon risks and risk mitigation strategies (roughly 30 minutes for each intersection point). A discussion of uncertainties and ramifications related to the intersection point may help drive that discussion. During the discussion, the facilitator should visually display or highlight the current intersection point to help keep participants on topic. For example, the facilitator can draw a red rectangle around the current intersection point on the virtual whiteboard.

Facilitator Talking Points	▪ The goal for the facilitator is to keep the discussion as free flowing as possible in order to identify a variety of potential risks and mitigation strategies.
	  ○ It is okay for participants to disagree.
	  ○ Generating new and different ideas is more important than building consensus.
	▪ As an example, let's assume that a majority of participants chose the intersection point 5C for the topic Anonymity and Privacy (the intersection of the column "Provide Identity Management and Associated Trust Support Services" and the row "Abuse of user data sharing practices"; see Appendix B).
	  ○ Start with the person(s) who voted for the intersection point to identify a risk that could arise from the abuse of data sharing practices that could affect services to assure trust in identity management.
	  ○ Ask that person and others to expand on the risk. Why is it relevant? Why is it important? What are the implications/consequences if the risk is unchecked?
	  ○ Finally, have participants identify plausible mitigation strategies to counter this risk.

	○ Then solicit participants to identify another risk. ○ Continue in this fashion for 30 minutes and then move on to the next intersection point. ▪ Here are some general questions for each risk identified: ○ Are there specific implications at the local, state, regional, or federal level? ○ Are there specific implications for one or more CI sectors? ○ Are there specific implications for CISA? ○ Are there specific implications for the public? ○ Are there current activities being undertaken to address this risk? ○ Are there best practices to build on? ○ How do you view/understand [insert driver of change]? How might this driver affect other drivers or trends on the matrix? What cascading impacts might occur that would link back to concerns for CI security and resilience? ○ Is there a precedent for or example of the risk mitigation strategy you are proposing? ○ Is the risk changing over time? How has the risk evolved? ▪ Encourage participants to use the platform's chat function as a means for them to ask follow-up questions to each other, expand on statements made, and provide links to additional information. The chat can also serve as a parking lot for ideas. Facilitators should scan through the chat comments and, as appropriate, introduce comments into the discussion.

IV. **FINAL THOUGHTS AND WRAP-UP** (4:45–5:00pm): The facilitator will ask participants to highlight their key takeaways from the risks and risk mitigation strategies that they identified. Additionally, the facilitator will briefly inquire about any NCFs or drivers of change that were not addressed by any of the six intersection points selected.

Breakdown	1. Ask participants for key takeaways. 2. Identify and discuss any NCFs or drivers of change not covered. 3. Make note of participant interest in pursuing follow-up activities (e.g., sharing results and attendee contact information, building out top priority areas from the discussion, obtaining input and assistance on unaddressed portions of the matrix chart)
Facilitator Talking Points	▪ Some wrap-up questions for participants include the following: ○ What were your key takeaways? ○ What was the most surprising or unexpected risk or risk mitigation strategy identified? ○ What was the most enjoyable part of this workshop? The least? Are there any improvements you would suggest? ▪ Look for any driver of change or NCF not chosen by any participant. Is there any reason why this driver or NCF wasn't selected?

APPENDIX A: DATA STORAGE AND TRANSMISSION

Topic description: Data creation is growing at an increasing rate, placing greater importance on secure data storage and transmission. Data access, integrity, and confidentiality are critical to accomplishing national objectives, including economic growth, improvements in medicine, public health, and public safety, and dominance in key emerging technologies (e.g., artificial intelligence). The nation must also guard against potential risks, including breaches, privacy violations, algorithm bias, misuse of data, and loss of public trust. Approaches to data—what's considered fair, appropriate, and desirable—can vary greatly among countries and lead to competitive advantages. Without a better understanding of these differences, the U.S. may be inadvertently reducing its ability to use data as a value driver and its competitiveness internationally.

Drivers of Change	National Critical Functions					
	1. Provide Internet-Based Content, Information, & Communication Services	2. Provide Internet Routing, Access, and Connection Services	3. Protect Sensitive Information	4. Operate Core Network	5. Provide Information Technology Products and Services	6. Provide Identity Management & Associated Trust Support Services
A. Increasing volume of data						
B. Inadequate access controls						
C. Reliance on cloud computing						
D. Rise in the number of Internet of Things devices						
E. Data management and quality issues						
F. Increasing number of cyberattacks & changing tactics						
G. International competition/conflict						
H. Remote work						

APPENDIX B: ANONYMITY AND PRIVACY

Topic description: Maintaining the balance between identity verification—for purposes such as voting, disease-related contact tracing, and law enforcement—and protecting anonymity is becoming increasingly challenging. Online activity and tracking, machine learning, facial recognition, data aggregation, and third-party data brokers present evolving threats to individual control of data and privacy. Meanwhile, recent data privacy laws and regulations, such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act, have redefined what constitutes personal data.

Drivers of Change	National Critical Functions					
	1. Protect Sensitive Information	2. Preserve Constitutional Rights	3. Enforce Law	4. Provide Information Technology Products and Services	5. Provide Identity Management & Associated Trust Support Services	6. Provide Internet Based Content, Info, & Communication Services
A. Improper security protocols						
B. Ubiquitous and unregulated data collection, brokering, and aggregation						
C. Abuse of user data sharing practices						
D. Technological advancements						
E. Legislation						
F. Insufficient data governance						
G. IT/OT convergence						

APPENDIX C: TRUST AND SOCIAL COHESION

Topic description: Social cohesion is commonly defined as citizens' belief that they share a moral community or common focus on societal well-being with one another, their governing bodies, and other institutions. This belief generally leads to trust. Social cohesion provides a source of potential risk to critical infrastructure and cybersecurity as well as a tool to mitigate that risk. Numerous factors can influence the degree of social cohesion, or sense of belonging, within a community and the effect of that cohesion on individual and community behavior and overall security. For example, Americans and critical infrastructure owners look to institutions to perform important functions such as ensuring public safety and supporting the secure and reliable delivery of NCFs. The ability or inability to provide these functions reliably—whether real or perceived—can affect public trust, diminish faith in function, and have deleterious impacts on national security. Exploring how emerging risks to critical infrastructure and cybersecurity and potential mitigation strategies affect social cohesion, positively and negatively, will give us useful insight into the associated individual and community responses and their impact on critical infrastructure and cybersecurity risk management. Such analysis may expose unanticipated threats and vulnerabilities caused or exacerbated by reduced social cohesion or challenges to potential response activities. Alternatively, we may illuminate underappreciated systemic resilience and identify opportunities for high-impact intervention resulting from increased social cohesion.

Drivers of Change	National Critical Functions					
	1. Enforce Law	2. Operate Government	3. Conduct Elections	4. Prepare for and Manage Emergencies	5. Support Community Health	6. Provide Public Safety
A. Declining trust in law enforcement						
B. Evolving means of communication						
C. Rise in disinformation						
D. Social media-enabled echo chambers						
E. Declining trust in impartial media						
F. Spread of protectionist polices						
G. Foreign ownership of key supply chain routes						