Joint Cyber Defense Collaborative

Russia-Ukraine Tensions Cyber Defense Plan Tabletop Exercise



2022-NTC-00218-000010

Exercise Facilitators

(b)(6)

U.S. Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

2022-NPPD-00218-000011

Welcome and Introductions

Interagency Partners

(b)(7)(D)

Private Sector Partners

(b)(7)(D)

(b)(7)(D)

2022-NPPD-00218-000012

Exercise Schedule

Time (EST)	Activity
12:00 p.m. – 12:15 p.m.	Welcome and Introductions
12:15 p.m. – 12:30 p.m.	Threat Brief
12:30 p.m. – 1:45 p.m.	Module One: Phase 1 & 2
1:45 p.m. – 2:00 p.m.	Break
2:00 p.m. – 3:15 p.m.	Module Two: Phase 3
3:15 p.m. – 3:45 p.m.	Hot Wash / Closing Comments

2022-NFO-00213-000013

OPENING REMARKS

2022-NFC-00218-000014

THREAT BRIEF

Security Protocol

- **Traffic Light Protocol (TLP): TLP:RED**
  - Not for disclosure, restricted to participants only.
  - Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
- For reference purposes and additional information on TLP: https://www.us-cert.gov/sites/default/files/tlp/tlp-v1-letter.pdf

Housekeeping Information

- Stay Muted Unless Speaking
- Unclassified Discussion Only
- Use Raise Hand Feature
- Use of Chat Encouraged

2022-NFO-00218-000017

Exercise Guidelines

- Open, no-fault, low-stress discussion
- Scenario
  - Only a snapshot
  - Focus on how you would respond if this happened, and not whether this could happen
- Post-Exercise
  - Feedback Form

2022-NPPD-00218-000018

Exercise Purpose

To examine the coordination, collaboration, information sharing, and response capabilities of JCDC partners in response to a significant cyber incident impacting U.S. critical infrastructure stemming from ongoing political tensions.



2022-NFO-00218-000019

Exercise Objectives

(b)(7)(E)

2022-NPPD-00243-000020

EXERCISE DISCUSSION

2022-NFC-00218-000021

MODULE 1

2022-NFC-00218-000022

February 21, 2022

- Open source imagery indicates Russian military forces are now, according to many analysts, 'in final preparations for invasion.'
- While striking a conciliatory tone earlier in the week, rhetoric from Russian diplomats and officials has hardened, indicating that any consideration of Ukraine joining NATO is 'no longer feasible.'
- While there are no known threats or intelligence to indicate imminent attacks against U.S. infrastructure, government and cybersecurity researchers believe that Ukrainian critical infrastructure nodes will be targeted as a precursor to kinetic attacks.

2022-NPPD-00218-000023

Discussion Questions

1. How is informal and formal information sharing between JCDC partners occurring at this point?
   a. What information would interagency partners request from industry partners?
   b. What information would industry partners request from interagency partners?
2. What line of effort would you prioritize?
3. Is joint messaging appropriate?
4. Discuss key operational coordination activities such as planned or potential defensive actions and outreach to targeted sectors.

2022-NFO-00218-000024

February 24, 2022

- News sources report that Russian military forces have entered Ukraine from the north and east. It is expected Russian forces will enter the capital within 48 hours.
- Reports indicate that many Ukrainian government offices, media outlets, IT and communications providers, and major financial institutions are experiencing severe disruptions, likely due to destructive malware. In some cases, secondary impacts occur to partner networks outside of Ukraine.
- U.S. and NATO allies denounce Russia's actions and indicate various sanctions will be swiftly imposed.
- While there is no specific targeting of U.S. infrastructure, dark web analysis indicates several Russian-based criminal actors will increase opportunistic attacks globally.

2022-NFO-00218-000025

Discussion Questions

(b)(7)(E)

2022-NPPD-00243-000026

BREAK

2022-NTC-00218-000027

MODULE 2

2022-NFC-00218-000028

February 27, 2022

- Two days ago, the U.S. and several NATO allies imposed sweeping sanctions against Russia.
- Beginning yesterday, several U.S. energy and water utilities reported anomalous activity on control system networks; several types of network devices are failing or nonresponsive. No stoppage of services has occurred, but several operators have implemented manual operations while investigations are underway.
- Several U.S. financial institutions report isolated outages to several internet-facing servers. Initial indications are that destructive malware was utilized.

2022-NPPD-00218-000029

Discussion Questions

(b)(7)(E)



2022-NPPD-00218-000030

March 1, 2022

- Russian military incursions continue into Ukraine, while additional crippling cyber attacks occur to Ukrainian civilian infrastructure.
- Investigations at impacted U.S. utilities discover, with further analysis done by cybersecurity vendor “Sector 7,” malicious embedded code on network devices made by two vendors.
- Analysis of malware found on several servers owned by U.S. financial institutions, coupled with analysis from Ukrainian sources, indicate similar code structure.

Discussion Questions

(b)(7)(E)

2022-NPPD-00243-000032

HOTWASH

2022-NFC-00218-000033

Hotwash

- Strengths
- Areas for Improvement
- Additional Comments

(b)(7)(E)

2022-NPPD-00218-000034

CLOSING COMMENTS



For more information:

CISA.gov

CISA Exercises:

(b)(6)

JCDC Partnerships:

CISA.JCDC@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

(b)(5)

(b)(5)

(b)(5)

Joint Cyber Defense Collaborative (JCDC) Russia-Ukraine Cyber Defense Plan: Lessons Learned

August 19, 2022

OVERVIEW

The JCDC Russia-Ukraine Cyber Defense Plan was developed in response to the Russian invasion of Ukraine, which sparked concern over threats to United States-based critical infrastructure. The Plan was developed jointly with the Cybersecurity and Infrastructure Security Agency's (CISA) JCDC, interagency, and Alliance partners with the purpose of providing a framework for collaborative action, to include: 1) coordinating partner actions that mitigate impacts to U.S. critical infrastructure in the event of an attack; 2) building and enforcing resilience of U.S. critical infrastructure; and 3) establishing channels and processes that ensure timely and effective collaboration.

The Plan was developed during the January-February 2022 timeframe with JCDC interagency and Alliance partners. During the February-May 2022 timeframe, JCDC was postured at Phase 2 of the Plan, which meant lowered thresholds for information sharing and continued monitoring of the risk environment. On June 2, 2022, JCDC shifted to Phase 4 with the understanding that lowered thresholds for reporting and sharing would continue through steady-state processes due to the "new normal" heightened risk environment.

The intention of this document is to capture lessons learned from the development and execution processes related to the Plan. It enumerates successes and challenges that will inform future JCDC Planning projects.

LESSONS LEARNED: BEST PRACTICES

During the **development** of the Plan, CISA JCDC noted several best practices:

1) The Russia-Ukraine Core Planning Team (CPT) quickly convened and collaborated virtually using unclassified out-of-band (OOB) networks on the development of a plan based on credible intelligence provided by interagency partners.

2) The Plan captured and organized multiple ongoing efforts throughout CISA and the JCDC collaborative structure, including ongoing briefings, information sharing sessions, and public messaging.

3) The planning process brought Sector Risk Management Agencies (i.e., Department of Energy, Department of Treasury) into the development stage.

During the **execution** of the Plan, CISA JCDC noted several highlights:

1) JCDC leveraged Slack channels to disseminate Russia-related information rapidly to members of the CPT, as well as to relevant non-Alliance partners.

2) CISA and interagency partners provided TS/SCI briefings to the Alliance, which provided helpful context for plan development. Additionally, unclassified briefings were provided to complement plan development through the Department of Homeland Security's Intelligence & Analysis component.

3) JCDC exercised the Plan through a snap Tabletop Exercise (TTX), which was based on previous Russian targeting of U.S.-based critical infrastructure. The TTX provided a better understanding of roles and responsibilities amongst partners and enabled the refinement of the Plan.

LESSONS LEARNED: CHALLENGES

During the **development** of the Plan, CISA JCDC noted several challenges:

1) The Plan's initial "TLP: Red" marking caused confusion and precluded participants from sharing within their organization. This resulted in a change to "TLP: Amber" markings.

2022-NPFO-00215-000007

2) The "TLP: Amber" marking was an improvement, but confusion still existed around the extent to which the Plan could be shared for a more deliberate purpose.

3) The Plan was developed on an ad-hoc basis rather than through a repeatable process.

4) The usefulness of the Plan was limited for some partners because of the lack of specificity associated with the actions described in the Plan.

During the **execution** of the Plan, CISA JCDC noted several challenges:

1) The participants in the Slack channels were not always the most relevant CPT and operator-level members, resulting in occasional delayed coordination.

2) Collaborating from both the CISA OOB and standard CISA unclassified systems confused some partners and resulted in information crossover from both Alliance and interagency partners.

3) Some industry partners received duplicative high-side briefings which were burdensome to attend.

4) The scenario and format of the TTX lacked relevant and tailored content for the participants. As a result, it was not effective in validating the Plan. Challenges with the development of the exercise were largely attributed to the limited amount of time to organize a quick-turn TTX and the lack of established processes to support its execution.

LESSONS LEARNED: WHERE DID WE GET "LUCKY"

During the development of the Plan, CISA JCDC noted several instances of "luck". "Getting lucky" is defined as factors that positively impacted JCDC joint response that are environment-based and likely not replicable:

1) Though there were risks associated with blowback from supporting Ukraine, the U.S. does not appear to have been the main target of Russian aggression during the Plan's initial rollout.

2) An unprecedented amount of information and intelligence was available at the unclassified level.

RECOMMENDED IMPROVEMENTS

CISA JCDC is tracking the following proposed improvements:

Table 1: Recommendations

(b)(5)

2022-NPFO-00215-000008

(b)(5)

CONCLUSION

CISA JCDC will work to incorporate the above lessons learned into future JCDC planning efforts. The most immediate updates will be made to the JCDC Enhanced Posture and Operational Collaboration (EPOC) Framework – the EPOC will absorb the functions of the Russia-Ukraine Cyber Defense Plan and be used in response to potential Russian malign activity against U.S.-based critical infrastructure.

2022-NPFO-00215-000009



Joint Cyber Defense Collaborative

Cyber Defense Plan: Russia-Ukraine Tensions

Cybersecurity Division
Cybersecurity and Infrastructure Security Agency

Version 1.0
February 2022

DISCLAIMER: This document is marked TLP:RED--Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person. For more information about the Traffic Light Protocol (TLP), see Appendix B.

2022-NPFO-00215-000038

CONTENTS

Summary 3
Purpose 3
Planning Considerations 4
Operational Phases 5
Phase 1: Preparatory Activities 5
Phase 2: Proactive Risk Management 5
Phase 3: Response Coordination 5
Phase 4: Demobilization 5
Phase 5: Measure Effectiveness 5
Thresholds 6
Lines of Effort and Action 7
Phase 1: Preparatory Activities 7
Phase 2: Proactive Risk Management 10
Phase 3: Response Coordination 11
Phase 4: Demobilization 13
Phase 5: Measure Effectiveness 13
Appendix A: Acronym and Definitions 15
Appendix B: Traffic Light Protocol 16
Appendix C: Critical Information 17
Overview 17
Pre-Incident Critical Information 17
Response Coordination Critical Information 18
Additional Network Framing Questions 19
Network Overview 19
Network Design 19
Cyber Threat 19
Impact 20
Cyber Vulnerability/Hygiene 20
Network Weaknesses 20
Network Supporting Infrastructure 20

Joint Cyber Defense Collaborative Cyber Defense Plan: Russia-Ukraine Tensions

SUMMARY

Nation- and non-nation states are in perpetual competition. As competition becomes more contested, geopolitical tensions increase the risk of sudden conflict both above and below the use of armed force. This risk includes an increased threat in and throughout cyberspace, raising the prospect of intentional or unintentional cyber impacts to critical infrastructure that could disrupt national critical functions (NCFs). It is prudent to undertake proactive planning to increase and adjust Joint Cyber Defense Collaborative (JCDC) activities accordingly.

Recent Russian military deployments have sparked global concerns of an imminent military invasion of eastern Ukraine. The DHS Office of Intelligence and Analysis (I&A) Cyber Mission Center has assessed that Russia would consider initiating a disruptive or destructive cyberattack against the United States—as distinct from its ongoing espionage and influence operations—if the Kremlin perceives that a U.S. or NATO response threatened Russia's national security. This assessment is based on recent Kremlin messaging, past and present Russian activities in cyberspace related to U.S. critical infrastructure, Russia's demonstrated intent and capability to disrupt and destroy critical infrastructure in other countries, and its government's heavy focus on "information confrontation" in conducting foreign policy. DHS assesses that Russia probably has a high threshold for conducting disruptive or destructive cyberattacks against the United States, considering past instances of U.S. and NATO support for Ukraine. Based upon I&A's assessment, the JCDC believes that Russia's activities warrant the development of a proactive cyber defense plan.

PURPOSE

This plan provides a framework for collaborative action to:

- Mitigate harmful impacts to U.S. critical infrastructure and the U.S. economy from Russian cyber operations taken in retaliation to U.S. and allied policy related to Ukraine;
- Weaken Russia's cyber deterrent and thereby maximize options available to U.S. decision makers for responding to Russian aggression against Ukraine; and
- Demonstrate the resilience of U.S. critical infrastructure to attack by foreign adversaries.

Specific activities intended to achieve the above end state include:

- Identify JCDC Alliance partner capabilities and personnel that may be relevant to support preparatory and response coordination activities;
- Specify how JCDC Alliance partner capabilities will be utilized for unified action before, during, and after a cyber incident that has the potential to damage U.S. critical infrastructure;

- Formalize methods and thresholds for information sharing among JCDC Alliance partners; and
- Enhance JCDC communication to key partners, including: Sector Risk Management Agencies (SRMAs) and critical infrastructure owners and operators; state and local governments; international partners, and the public.

PLANNING CONSIDERATIONS

This plan provides a framework for the following collaborative action:

- JCDC Alliance partners will actively engage in collaborative planning and execution to address increased cyber risks from geopolitical tensions.
- Industry activities undertaken as part of JCDC will be voluntary. Where appropriate, JCDC Alliance partners will discuss relevant legal processes.
- No one organization will have timely, holistic insight; therefore, robust sharing of information is essential to effective joint cyber defense of NCFs.
- Implementation of this plan will be coordinated with the execution of other national plans to provide an integrated whole-of-nation response. Individual JCDC Alliance partners will take cyber defense actions within their unique authorities.
- An isolated incident affecting a single element of critical infrastructure could expand and/or have cascading impacts across critical assets and sectors. As such, incident identification under this plan will depend on subjective assessments of potential consequences of adversary activity.
- Participants will bear their own costs and risks for participation in the JCDC and in carrying out any coordinated actions.
- Ongoing planning efforts will consider potential effects to U.S. supply chains and U.S.-based global companies that operate critical infrastructure should NATO or other U.S. allies be attacked.
- Ongoing planning efforts will consider the potential actions of other adversaries and criminal groups should U.S. critical infrastructure be targeted.
- Ongoing planning efforts will consider response actions given the likelihood of significant and unanticipated attacks using previously unidentified vectors and vulnerabilities.

OPERATIONAL PHASES

In executing cyber activities to defend U.S. critical infrastructure amid elevated Russia-Ukraine tensions, JCDC will organize its cyber defense operations into five phases, which are aligned to eight planning objectives. Some activities may transcend all operational phases, and those that are implemented during earlier phases might continue during later phases. These phases are:

Phase 1: Preparatory Activities

- **Objective 1:** *Information Sharing* – Consistent with applicable law, JCDC Alliance partners lower thresholds to timely, robust sharing of information, intelligence, and analysis among JCDC Alliance partners throughout the duration of the operation.
- **Objective 2:** *Joint Messaging* – JCDC Alliance partners support CISA messaging to critical infrastructure stakeholders to improve cybersecurity.
- **Objective 3:** *Operational Coordination* – JCDC interagency partners are postured to defend against malicious cyber activities threatening U.S. critical infrastructure or NCFs. JCDC industry partners are positioned to provide insight and coordinate defensive activity to protect NCFs.

Phase 2: Proactive Risk Management

- **Objective 4:** *Active Monitoring* – JCDC Alliance partners warn of, identify, and support USG attribution of malicious activity and take proactive action to improve the collective defensive posture.
- **Objective 5:** *Proactive Risk Reduction* – JCDC supports risk management to reduce potential impacts to critical infrastructure.

Phase 3: Response Coordination

- **Objective 6:** *Response Coordination* – JCDC provides coordinated insight and voluntary defensive actions to protect NCFs.

Phase 4: Demobilization

- **Objective 7:** *Transition* – JCDC efficiently and effectively transitions focus from response coordination to steady state priorities.

Phase 5: Measure Effectiveness

- **Objective 8:** *Continual Improvement* – JCDC government and industry partners understand the impact of defensive activities taken and are better postured for future defensive activities.

THRESHOLDS

CISA will make every attempt to consult and collaborate with JCDC Alliance partners to obtain consensus regarding collective action through the JCDC construct. CISA leadership retains the authority to implement this plan and transition between phases should unanticipated conditions preclude further pre-activation consultation. Any JCDC Alliance partner can suggest activation of this plan or movement from one phase to another phase to CISA. Upon activation of this plan, CISA will communicate with all JCDC Alliance partners to initiate and coordinate activities.

The following will serve as common thresholds for CISA leadership, in coordination with JCDC Alliance partners, to transition between phases:

- **Phase 1** may be activated in the event that geopolitical events increase the potential for cyber incident(s) and pose demonstrable risk to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people
- **Phase 2** may be activated during heightened probability of a significant escalation in geopolitical events or in the event that a significant escalation poses particular risk to U.S. critical infrastructure.
- **Phase 3** may be activated in response to malicious cyber activity resulting from geopolitical tensions that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. Cyber incidents may include:
    - **Compromise of U.S. critical infrastructure:** Intelligence and digital forensics confirm repeated and unusual targeted attempts or successful intrusions from suspected Russian actors affecting the administrative or operational networks of one or more critical infrastructure owners and operators. Malicious actors obtain access that could enable persistence inside some target networks, but critical infrastructure systems and services remain fully operational. (Example: Adversaries deploy malware payloads inside corporate or operational networks to obtain persistent access to those systems.)
    - **Isolated Disruption of U.S. critical infrastructure:** Multiple elements of critical infrastructure experience temporary and isolated loss of system functionality or services that pose some risk for business continuity in the event of adversary escalation. (Example: Malware directly or indirectly disrupts access to a limited number of non-mission critical systems or services.)
    - **Widespread Disruption of U.S. critical infrastructure:** One or multiple elements of critical infrastructure or their dependencies experience temporary or sustained loss of system functionality or services that pose a direct threat to business continuity for initial victims and dependent organizations down the supply chain. (Example: Sustained disruptions affecting cloud-based services prevent thousands of businesses from conducting remote work.)

- **Irreversible Damage to U.S. critical infrastructure or Human Life:** One or multiple elements of critical infrastructure experience irreversible damage to infrastructure and operations, triggering cascading effects across multiple sectors. Effects might include permanent loss of data, physical destruction of cyber-physical systems or their dependent components, and physical injury to people. (Example: Malware overrides industrial safety systems at a natural gas plant, causing physical destruction that injures workers and disables the plant for the foreseeable future.)

- **Phase 4** will begin in the event that geopolitical events diminish to the point that they no longer meet Phase 1 criteria.
- **Phase 5** will be initiated immediately following the conclusion of Phase 4 demobilization activities.

LINES OF EFFORT AND ACTION

The following Lines of Effort (LOEs) organize preparatory activities and joint actions that JCDC will jointly undertake to protect, detect, respond to, and recover from cybersecurity threats that pose a potential risk to critical infrastructure or national interests.

Phase 1: Preparatory Activities

LOE 1: *Information Sharing* – Coordinate with JCDC Alliance partners and the federal government to share information and intelligence as broadly as possible. (JCDC All).

- **Action 1.1:** Engage Intelligence Community (IC) to provide context on adversary activities. (JCDC Interagency)
  - **Action 1.1.1:** Establish an IC cell led by DHS I&A to support the duration of the operation. (JCDC Interagency)
  - **Action 1.1.2:** Develop intelligence requirements to support leadership decision making and streamline information sharing efforts. (JCDC Interagency)
- **Action 1.2:** Collaborate with Interagency Partners and applicable SRMAs.
  - **Action 1.2.1:** Convene JCDC interagency partners and SRMAs to share intelligence and potential government actions. (JCDC Interagency)
- **Action 1.3:** Collaborate with JCDC Industry Partners.
  - **Action 1.3.1:** Establish an active information sharing mechanism (e.g. Slack), or mechanisms, with JCDC Alliance partners. Agree to lower thresholds for threat and incident information sharing consistent with applicable laws during a heightened state of operational readiness. (JCDC All)
    - **Action 1.3.1.1:** Identify relevant JCDC Alliance partner customer lists. Share such customer lists with JCDC Interagency partners, as practicable and allowable. (JCDC Industry)

        - **Action 1.3.1.2:** Aggregate customer lists described in Action 1.3.1.1 and share with JCDC Alliance and Specialist partners as permitted by JCDC Alliance contributors. (JCDC Interagency)
        - **Action 1.3.1.3:** Identify actionable data/analysis and share among all JCDC Alliance partners. Actionable information may include warning of anomalous activity, signatures, indicators of compromise (IOCs), tactics, techniques and procedures (TTPs), analytic products, defensive measures, and mitigations. (JCDC All)
        - **Action 1.3.1.4:** Integrate private sector threat intelligence providers into I&A-led IC cell to the extent allowable. (JCDC All)
        - **Action 1.3.1.5:** Evaluate current available information and discuss whether joint messaging is appropriate. (JCDC All)
    - **Action 1.3.2:** Engage JCDC Alliance partners and critical infrastructure sectors to brief threat activity and encourage coordinated preparation. (JCDC All)
        - **Action 1.3.2.1:** Leverage list of JCDC industry partners with clearances who can support classified planning and response actions. Utilize CISA headquarters to host cleared JCDC Alliance partners for classified briefings/attend classified meetings. Whenever possible, provide unclassified tearlines for use. (JCDC All)
        - **Action 1.3.2.2:** Approve standardized briefing document describing JCDC origins, purpose, and rationale for requesting information on a voluntary basis from JCDC Industry customers and other potential victims. (JCDC All)
- **Action 1.4:** Identify and collect information sharing-related lessons learned for the Phase 5 After Action Report (AAR). (JCDC All)

LOE 2: *Joint Messaging* – Strengthen proactive cybersecurity posture of critical infrastructure partners. (JCDC All)

- **Action 2.1:** CISA to convene JCDC Alliance partners to discuss relevant cyber threat and cyber defense information and jointly plan coordinated messaging that meets the needs of critical infrastructure partners. (JCDC All)
    - **Action 2.1.1:** Leverage existing meetings with key stakeholders and/or customer sets to amplify messaging. (JCDC All)
    - **Action 2.1.2:** Develop a list of pre-existing or incident-specific free tools and services that federal agencies and private sector entities (to include JCDC Alliance partners and beyond) that CISA can provide to a set of critical sectors or entities that CISA has identified as high risk, based on criticality, lack of existing resources, and threat model. (CISA)
    - **Action 2.1.3:** Aggregate and amplify JCDC Alliance partner messaging.

- **Action 2.2:** Collect and evaluate available cyber threat and cyber defense information to inform joint messaging. (JCDC All)
- **Action 2.3:** Identify relevant audiences and determine publication processes, timelines, and markings. (JCDC All)
- **Action 2.4:** Create, produce, synchronize, and disseminate specific JCDC products. (JCDC All) Messaging audiences will include:
    - State, local, tribal, and territorial (SLTT) governments, Federal Civilian Executive Branch (FCEB) entities, critical infrastructure owners and operators and SRMAs. See Appendix B for an explanation of the Traffic Light Protocol (TLP) and how CISA shares information with various stakeholders.
    - Broader partners and the public: These products are normally published on the CISA.gov website and are made available to all stakeholders.
- **Action 2.5:** Identify and collect messaging-related lessons learned including feedback on product quality and utility, for the Phase 5 AAR. (JCDC All)

LOE 3: *Operational Coordination* – Coordinate planned and potential defensive actions to respond to and minimize the impact of malicious cyber activities. (JCDC All)

- **Action 3.1:** Leverage JCDC point of contact list to ensure that 24/7 operational communications are open with JCDC Alliance partners. (JCDC All)
- **Action 3.2:** Convene working sessions with JCDC Alliance partners to discuss intelligence background and jointly plan potential coordinated actions. (JCDC All)
    - **Action 3.2.1:** Identify JCDC Alliance partners' technical and organizational capabilities and knowledge base. (JCDC All)
    - **Action 3.2.2:** Work with JCDC Alliance to compile a list of JCDC Specialist partners that can support JCDC response coordination in targeted sectors and coordinate with these partners. (JCDC All)
    - **Action 3.2.3:** Evaluate current available information and discuss what joint messaging is appropriate. (JCDC All)
    - **Action 3.2.4:** Establish bilateral channels if JCDC Alliance partner needs to evaluate information with CISA prior to its being released to others in JCDC.
- **Action 3.3:** Employ several software tools, including but not limited to Slack, to facilitate resilient information sharing with key industry partners and appropriate interagency participation. Leverage automated indicator sharing mechanisms when possible. Pre-deploy additional channels and tools based on operational need. (JCDC All)
    - **Action 3.3.1:** Establish four separate channels of communication for (1) pre-incident planning; (2) real-time dialogue for rapid issue resolution–whether during steady state or incident response; (3) automated data exchange; and (4) backup communications channel reliant on separate infrastructure. (JCDC Interagency)

- **Action 3.3.2:** Employ shared calendar with JCDC Alliance partners to clarify steady-state tempo of operations and coordinate participation of relevant SMEs. (JCDC All)
- **Action 3.3.3:** Socialize standard operating procedures regarding use of communication channels. (Comms SOPs are currently under development by the JCDC Planning Office). (JCDC All)

- **Action 3.4:** Identify and collect operational coordination-related lessons learned for the Phase 5 AAR. (JCDC All)

Phase 2: Proactive Risk Management

LOE 4: *Active Monitoring* – Monitor Internet activity, adversary actions, stakeholder networks, allied actions, and overall geopolitical environment to identify indicators of escalation, potential retaliatory activity, and/or potential opportunistic activity by third parties. (JCDC All)

Consistent with applicable law, partners lower thresholds to timely, robust sharing of information, intelligence, and analysis between JCDC Alliance partners throughout the duration of the operation.

- **Action 4.1:** Leverage visibility to monitor for adversary cyber activity. (JCDC All)
  - **Action 4.1.1:** Monitor intelligence for signs of cyber and non-cyber activity indications and warnings, and share information to the extent possible. (JCDC All)
  - **Action 4.1.2:** Monitor intelligence for signs third parties, including non-state groups as well as nation states other than Russia are seeking to opportunistically capitalize on tensions with their own malicious cyber activities, and share such information to the extent possible. (JCDC All)
- **Action 4.2:** Assess potential risk of activity that may counter defensive action, provide warning, and coordinate within JCDC to proactively initiate joint cyber defense planning when appropriate. (JCDC All)

LOE 5: *Proactive Risk Reduction* – JCDC supports risk management to reduce potential impacts to critical infrastructure. (JCDC All)

- **Action 5.1:** Take coordinated action to identify and promote adoption of real time improvements to build resilience. (JCDC All)
  - **Action 5.1.1:** Coordinate with IC to understand TTPs and capabilities of adversary and share with JCDC Alliance partners as possible. (JCDC Interagency)
  - **Action 5.1.2:** Leverage JCDC Alliance partners and industry capabilities and resources on a voluntary basis to harden infrastructure and build resilience, such as blocking known malicious traffic. (JCDC All)
  - **Action 5.1.3:** Coordinate with SRMAs to prioritize readiness efforts based on risk and promote sector-specific mitigation measures. (JCDC All)
  - **Action 5.1.4:** Evaluate current available information and discuss what joint messaging is appropriate. (JCDC All)

- **Action 5.2:** Identify and collect lessons learned from proactive risk management activities for the Phase 5 AAR.

Phase 3: Response Coordination

LOE 6: *Response Coordination* – Coordinate response and defensive support to counter and minimize impact from malicious cyber activities. (JCDC All)

- **Action 6.1:** Develop communications and defensive activity rhythm with all JCDC Alliance partners, including predictable cycles of standardized reporting. (JCDC All)
    - **Action 6.1.1:** Convene snap JCDC Senior Advisory Council call to determine the JCDC's current understanding of the incident. (JCDC All)
    - **Action 6.1.2:** Convene snap JCDC Alliance partner call (JCDC All) to:
        - Develop a common operating picture across JCDC Alliance partners;
        - Refresh information sharing threshold expectations;
        - Discuss public messaging; and
        - Establish next steps and cadence for future discussions.
    - **Action 6.1.3:** Collect response guidance or activities that JCDC companies are taking on behalf of customers or recommending for the ecosystem. Broaden that guidance to a wider audience as a central repository. (JCDC All)
    - **Action 6.1.4:** If an incident causes physical impacts, coordinate with appropriate FEMA offices to support on-the-ground response as applicable. (JCDC Interagency)
- **Action 6.2:** Continue to share data, intelligence, and analysis across JCDC Alliance partners to identify and defend against malicious activity, coordinate response as possible, and triage victims for support. (JCDC All)
    - **Action 6.2.1:** Share incident scoring and analysis between JCDC Alliance partners, as possible. (JCDC All)
    - **Action 6.2.2:** Input IOCs/TTPs received through JCDC information sharing platforms into internal analysis and develop enriched products to redistribute to all JCDC partners for feedback. (JCDC All)
    - **Action 6.2.3:** Engage ISACs/ISAOs with direct insight into affected sectors and integrate proper POCs into JCDC operations. (JCDC All)
    - **Action 6.2.4:** Identify JCDC Industry customers that support critical but unaffected functions of impacted sector(s) for purposes of providing tailored guidance for enhanced protections. (Example: Russia disrupts aviation operations and several JCDC Industry partners support weather forecasting or ground control services.) (JCDC All)

- **Action 6.2.5:** Collect victim-specific list of already-deployed security measures, capabilities, and tools to focus delivery of technical assistance by JCDC Interagency or JCDC Industry partners. (JCDC All)
- **Action 6.2.6:** Share updated IOCs/TTPs–including context explaining malicious purpose–through appropriate platforms, including: timestamped network traffic information; network configurations; malware samples (not hashes of malware samples); specific vulnerabilities exploited on victim networks; affected products and services (make/model/version). When possible, align information to cyberattack frameworks, such as MITRE ATT&CK. (JCDC All)

- **Action 6.3:** If a Unified Coordination Group (UCG) is established, per Presidential Policy Directive 41, CISA will lead asset response for the federal government, and will serve as the touchpoint in the UCG for JCDC Industry partners.
  - **Action 6.3.1:** CISA will represent industry equities in UCG discussions, share incident information provided by JCDC Industry partners, and report UCG outputs to JCDC Industry partners for consumption or action to the extent possible. (CISA)
  - **Action 6.3.2:** CISA will coordinate messaging across UCG participants and all JCDC partners. (CISA)
  - **Action 6.3.3:** To the extent possible, JCDC Interagency partners may invite JCDC industry partners to participate in UCG processes and dialogue. (JCDC Interagency)
- **Action 6.4:** Coordinate prioritized joint actions. (JCDC All)
  - **Action 6.4.1:** Conduct regular sessions on a standard cadence (unclassified or classified), with JCDC Alliance partners to share information, plan, coordinate activities, and share feedback. (JCDC All)
  - **Action 6.4.2:** Identify and coordinate rapid development of software patches, mitigations, guidance, and best practices based on observed malicious activity. (JCDC All)
  - **Action 6.4.3:** Incorporate new data and intelligence into cybersecurity products and solutions and synchronize updates for partners. (JCDC All)
  - **Action 6.4.4:** Categorize victims, as possible, that have consented to identification or have been identified by CISA based on geographic location and sector, notify SLTT entities to amplify notification, facilitate the delivery of cyber defense support, and coordinate assistance. (JCDC All)
  - **Action 6.4.5:** Triage and coordinate targeted notification, in accordance with existing processes, when applicable (JCDC All) for:
    - Known victims;
    - Potential victims;
    - Owners of attacking infrastructure/domains/servers; and

        - Customers of services that are at risk of disruption.
    - **Action 6.4.6:** Regularly share practical and legal barriers to response activities to inform exigency/waiver reviews. (JCDC All)
    - **Action 6.4.7:** Continuously catalogue, as possible, services and infrastructure that have been or may be disrupted and incorporate list into relevant communications with proper protections. (JCDC All)
    - **Action 6.4.8:** Coordinate voluntary industry cyber defense support activities through the JCDC (JCDC All), including but not limited to:
        - Targeted cyber support to a geographic area or system(s) at issue;
        - Increased monitoring services to detect additional activity;
        - Provision of services to detect, protect, or recover integrity and availability of critical functions; and
        - Network maintenance activities, including customer account changes and managing network traffic.
    - **Action 6.4.9:** Evaluate current available information and discuss what joint messaging is appropriate during response coordination. (JCDC All)
    - **Action 6.4.10:** Regularly publish response activity updates shared by JCDC members. (JCDC All)
- **Action 6.5:** Identify and collect lessons learned from response coordination activities. (JCDC All)

Phase 4: Demobilization

LOE 7: *Transition* – Demobilize from incident response actions and enhanced operational posture to resume normal day-to-day operations. (JCDC All)

- **Action 7.1:** Coordinate with partners to communicate demobilization and transition to steady state priorities. (JCDC All)
- **Action 7.2:** Evaluate current available information and discuss what joint messaging is appropriate during demobilization. (JCDC All)
- **Action 7.3:** Identify and collect lessons learned from demobilization activities. (JCDC All)

Phase 5: Measure Effectiveness

LOE 8: *Continual Improvement* – Measure effectiveness of activities and identify gaps for future improvement. (JCDC All)

- **Action 8.1:** Combine Lessons Learned from previous Phases. (JCDC All)
- **Action 8.2:** Identify and collect additional lessons learned to improve future response activities through interviews and surveys. (JCDC All)

- **Action 8.3:** Develop and track measures of effectiveness to assess impacts of joint defense activities. Impacts will be assessed against the LOE-specific objectives identified in Section 3 of this plan. (JCDC All)
- **Action 8.4:** Aggregate lessons learned and recommendations into JCDC After Action Report (AAR) including prioritized implementation plan. (JCDC All)
    - **Action 8.4.1:** Review and approve AAR. (JCDC All)
    - **Action 8.4.2:** Implement JCDC-related changes. (JCDC All)
    - **Action 8.4.3:** Evaluate current available information and discuss what joint messaging is appropriate during or after the AAR process. (JCDC All)

APPENDIX A: ACRONYM AND DEFINITIONS

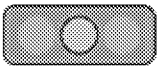
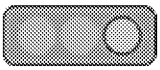
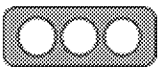
Acronym	Meaning	Definition
AAR	After Action Report	A detailed critical summary or analysis of a past event, created to re-assess decisions and consider possible alternatives for future scenarios.
CISA	Cybersecurity and Infrastructure Security Agency	CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.
IOC	Indicators of Compromise	An artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion
JCDC	Joint Cybersecurity Defense Collaborative	JCDC leads collaborative, public and private sector cyber defense planning, cybersecurity information fusion and analysis, and the purposeful dissemination of cyber defense guidance to reduce cyber risks to our National Critical Functions.
NCF	National Critical Functions	Functions of government and the private sector so vital to the United States 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.
SRMA	Sector Risk Management Agency	A federal department or agency designated by PPD-21 with responsibility for providing institu-tional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.
TLP	Traffic Light Protocol	A set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).
TTP	Tactics, Techniques, and Procedures	The behavior of an actor. A tactic is the highest-level description of the behavior; techniques provide a more detailed description of the behavior in the context of a tactic; and procedures provide a lower-level, highly detailed description of the behavior in the context of a technique.

APPENDIX B: TRAFFIC LIGHT PROTOCOL

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).

TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration. TLP is optimized for ease of adoption, human readability and person-to-person sharing; it may be used in automated sharing exchanges, but is not optimized for that use.

CISA JCDC and its partners can leverage TLP when sharing information with each other and external entities.

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

APPENDIX C: CRITICAL INFORMATION

Overview

Identifying specific types of critical information helps build situational awareness among all JCDC partners and facilitate timely and efficient decision-making processes related to JCDC's activation and execution of this plan. The intended audiences for these critical information types are JCDC interagency and industry partners.

Pre-Incident Critical Information

The following critical information types are aligned to Phases 1 and 2.

1. Any increase in malicious cyber activity targeting employees of U.S. businesses located overseas.
2. Any increase in cyber reconnaissance activity, initial intrusion-related activity such as phishing/spear phishing, or data theft related to critical infrastructure entities.
3. Any malicious activity toward Ukraine emanating from known malicious Russian APT actors.
4. Information on potential or suspected nation-state cyber operations and/or impacts and risks to U.S. critical infrastructure, including:
    - Any anomalous activity and information related to relevant Russian state and non-state actors (e.g., TTPs).
    - Attribution of activity to a Russian state actor and/or malicious cyber group.
5. Known trends and patterns regarding advanced persistent threat (APT) vulnerability exploitation, which can facilitate detection and remediation among likely vulnerable entities. Including:
    - CVEs
    - Software/Hardware (IT and OT/ICS)
    - Ports/Protocols
    - Known vulnerability vs. Zero Day
    - Vulnerability exploitation chain (if applicable)
    - Targeted Entity Characteristics (e.g., Sector, National Critical Function, size, etc.)
6. Any observed unexpected equipment behavior such as unexpected reboots of OT hardware and software, including digital controllers.
7. Any increase in targeting of specific critical infrastructure sectors emanating from known malicious Russian or unattributed actors.
8. Any dark web communications involving Eurasian cybercriminals regarding actions against U.S. or U.S. ally critical infrastructure.
9. Entities previously compromised by known Russian cyber actors, including attempts at reacquiring access.
10. Any previously unshared indicators related to malicious cyber activity that is unattributed but may be a nation-state, particularly Russia.
11. Any Russian targeting of networking devices—potentially via firmware or software updates—that might imply broader campaign-like attempts at accessing multiple victims.
12. Any instances in which known CVEs were patched but subsequently exploited.

Response Coordination Critical Information

The following critical information types are aligned to Phase 3.

13. Technical information and artifacts related to Russian APT actors, as well as criminal and non-state actors aligned with Russia. These technical artifacts may include:
    - Timestamped network traffic information
    - Network configurations and maps
    - Forensic images
    - Complete/partial malware samples
    - Specific exploited vulnerabilities on victim networks
    - Affected products and services
    - Raw logs (e.g., host, network, firewall, authentication, etc.)
    - Atomic IOCs (e.g., elements or fragments of data that cannot be broken down further or data that can individually indicate adversary activity)
    - Command and control infrastructure artifacts
    - Additional IOCs including domains, IP addresses, protocol ports, with timestamps
    - Other information as observed
14. Indicators of compromise (e.g., connections from nonstandard ports, creation of new privileges, after-hours network activity, etc.).
15. Any increased malicious cyber activity whether it is attributed APT or new un-attributed activity, against U.S. or U.S. ally critical infrastructure, to include telecommunication, financial, healthcare, transportation (such as aviation and rail), and energy (such as water, gas, and electric).
16. Increased attempts to exploit U.S. infrastructure (e.g., domains and servers) or providers (e.g., email, cloud storage, SaaS) by known malicious APT actors.
17. Any ICS/SCADA, or network security devices compromised by malicious APT actors.
18. Any efforts by known or suspected malicious APT actors to test exploitation capabilities, develop new malware, or otherwise prepare for cyber operations.
19. Any new coordinated inauthentic messaging attributed to overseas actors that spreads mis- or disinformation regarding cybersecurity or the security of critical infrastructure to U.S. audiences.
20. Observed network intrusion or penetration targeting related to Russian nation state APT actors, including when possible the following information:
    - Any information on critical infrastructure sector targeted, timeline, and geographic location
    - Any observed access to data storage or file systems
    - Any observed access to control systems
    - Any observed impact of the incident (e.g., to foreign policy, government operations, the economy, intellectual property, physical damage, reputation).
    - Any information sophistication of the perpetrator (tailored/unique tools, complex obfuscation, persistence).
    - Any strategic direction of the perpetrator (e.g., specificity of targeting versus target of opportunity).

- Any malware samples associated with the incident.
- Any adversary TTPs to include method of gaining initial access, lateral network movement, supply chain or insider tactics, attack payload deployment and triggering, persistence, obfuscation, ransom notes.
- Any observed tradecraft errors by the actor.

21. Any online infrastructure used by malicious cyber actors to carry out operations, to include IP addresses, domains, protocols/ports, certificates, cryptocurrency addresses.

Additional Network Framing Questions

These questions may be helpful when identifying relevant information on a targeted or compromised network. This information in many cases may not be available or sharable, but when applicable and possible can assist in contextualizing and understanding a cyber incident.

Network Overview

- What are the network's main functions?
- What are the major/critical network components?
- What are the mission critical **functions** on the network?
- What is the mission critical **information** on the network?

Network Design

- Are there network maps? Format?
- Number/locations of internet gateways?
- What is the bandwidth of the internal network? Potential sensor placement
- What is the bandwidth at the internet gateways? Potential sensor placement
- What are the number/location of hosts (Linux, Windows, etc.)?
- What are the number/location of infrastructure devices?
- Does the network/system have an ICS component?
- Does the network/system have a cloud presence?
- Does the network/system use any cloud providers for critical functions (email, ADFS, etc.)?
- How is the network segmented?
- What are the points of entry into the network (e.g., VPN)?
- Where are the major/critical network components located?
- Where are the mission critical functions located on the network?
- Where is the mission critical information located on the network?

Cyber Threat

- Why might someone target this network? Examples:
    - Capture critical and sensitive information
    - Gain indications and warning
    - Cause denial of service

- Modify/Usurp network functions
- Gain persistence

- What APT groups or individuals might be interested in this network?
- Are there any known incidents or activities that are of particular concern?
- Are there any details/reporting of adversarial targeting of the network, including IOCs?

Impact

- Does the pattern of malicious cyber activity suggest that specific critical programs or missions are the ultimate targets?
- What is the mission impact or risk if critical functions/information lose confidentiality, integrity and/or availability?

Cyber Vulnerability/Hygiene

- What security products are currently in use?
- Do you have periodical vulnerability scans of the network?
- Who is responsible for the network security?
  - In-house, remote/physical
  - Outsourced, remote/physical
  - Service Level agreements?
- How authentication is handled (MFA, tokens, passwords, etc.)?
- Is logging currently in place?
  - Who looks at these logs?
  - Are there network traffic logs?
  - Is there infrastructure device (firewall) logs?
  - Is there authentication logging?
  - Is there host logging?
  - How are incidents currently handled?

Network Weaknesses

- What are the network segments, components, and technology (1 – N segments) including: frequency of use, impact if attacked, weak points, network supporting infrastructure
- Power (frequency of use, impact if attacked, weak points)

Network Supporting Infrastructure

- Supply chain (frequency of use, impact if compromised, weak points)
- Personnel Security (frequency of use, impact if attacked, weak points)
- Physical/Facility Security (frequency of use, impact if attacked, weak points)

Joint Cyber Defense Collaborative

Implementation Resource B: General Schedule and Agenda Template Agenda for JCDC Ops Syncs

Updated April 2022

Overview

This document describes the objectives, logistics, and general schedule for recurring operational synchronization meetings ("Ops Syncs") between CISA and JCDC partners supporting the coordinated implementation of the JCDC Russia-Ukraine Tensions cyber defense plan.

Objectives

1. Establish a common understanding among all JCDC partners of the cyber risk landscape associated with the Russia-Ukraine crisis.
2. Discuss any associated operational impacts and/or impacts to National critical infrastructure.
3. Coordinate CISA and JCDC partner operational activities.

Conditions

Ops Syncs may be convened: (1) based on changes to the operating environment (i.e., an emerging threat); and/or (2) as recommended by CISA or any other JCDC partner.

Ops Sync Logistics and General Schedule

CISA will schedule Ops Syncs on a recurring basis, as required by operational demands; this may include multiple Ops Syncs per week. When scheduling an Ops Sync, CISA will send a meeting invitation to the primary points of contact for all JCDC partners; the meeting invitation will include meeting details and a notional agenda.

CISA will call the Ops Sync to order and ask participating JCDC interagency partners to provide a baseline threat assessment focusing on adversary activity and any associated operational impacts or impacts to national critical infrastructure. CISA will then ask JCDC Alliance and Specialist partners to offer their perspectives on the operating environment. Finally, CISA will facilitate a conversation between all meeting participants focused on coordinating operational activities. After the meeting, CISA will share a summary of conclusions with all meeting participants and note the date and time of the next Ops Sync.

Partner Roles

CISA

- Schedule Ops Syncs and manage the associated logistics (e.g., sending meeting invitations, developing agendas, and setting up conference lines).
- Share unclassified cyber threat intelligence.

- Facilitate discussion during Ops Syncs and document key questions, decision points, or actions.
- Identify key operational activities to be executed in JCDC Russia-Ukraine Tensions plan.
- Circulate a summary of conclusions to all meeting participants.

JCDC Partners

- Share unclassified cyber threat intelligence.
- Provide visibility into operational activities to support coordinated JCDC response efforts

Attachment

1. Ops Sync Agenda Template

(b)(5)