Critical Cyber Asset Identification and Prioritization Checklist

The intent of this checklist is to help emergency managers and other key stakeholders prepare to effectively respond to and recover from cyber incidents that disrupt critical services and operations. It lays out a general process for identifying and prioritizing a jurisdiction's critical cyber assets as part of the planning process.

For more information on this process and preparing for cyber incidents, please see the **Planning Considerations for Cyber Incidents: Guidance for Emergency Managers** available at fema.gov/plan.

Identification

□ Assemble a multi-disciplinary team which includes pertinent emergency management, legal, information technology, public safety, and private sector subject matter experts responsible for the jurisdiction.

□ Identify the critical services within the jurisdiction. Start with known critical services and then expand to identify related services. It may be beneficial to use community lifelines as a starting point.[1]

□ Develop a comprehensive list of critical infrastructure assets that support each critical service within the jurisdiction along with their owners and operators. This includes important assets:

  □ In the business operations of governance.

  □ In emergency response.

  □ To maintain public safety and order.

  □ For the economic stability of the jurisdiction or region.

  □ To provide medical care and public health services.

  □ For service of voice and/or data communication networks.

Examples of Critical Infrastructure

- Dispatch Centers
- Public Safety Answering Points (PSAPS)
- Emergency Operations Center
- Hospitals
- Water Treatment Plants

[1] Community lifelines are services that enable the continuous operation of critical government and business functions and are essential to human health and safety or economic security. They are the most fundamental services within a community that, when stabilized, enable all other aspects of society to function. For more information on community lifelines, visit: https://www.fema.gov/emergency-managers/practitioners/lifelines.

- □ To operate public messaging or warning systems.
- □ For providing basic essential services, such as water, electricity, or gas.

□ Meet with service owners and operators, service stakeholders, and any third-party service providers or vendors for identified critical infrastructure assets and discuss:

- □ Critical services and operations.
- □ Upstream, internal, and downstream dependencies.
- □ Cyber infrastructure (both internal and external to the organization) required to maintain critical services and operations.
- □ Likely consequences of service interruptions.
- □ How to gain situational awareness of the status and operational readiness of critical services during an incident.

Examples of Critical Cyber Infrastructure

- ▪ Core switch(s)
- ▪ Records Management System (RMS) software
- ▪ Public utility SCADA systems, (e.g., water delivery)
- ▪ Radio communication systems

□ Develop a comprehensive list of critical cyber infrastructure assets that support critical services and operations within the jurisdiction.

□ Compile the information obtained and create a critical services and dependencies inventory. The inventory captures the critical services, infrastructure, assets, associated owners and operators, other key personnel, and the dependencies among systems.

Prioritization

□ Develop a methodology and/or scoring mechanism to assess how critical each cyber infrastructure asset is for operations. A ***sample*** for scoring critical cyber infrastructure assets is available on the following pages.

□ Meet with service owners, operators, and relevant stakeholders to:

- □ Review each critical cyber infrastructure asset using the identified methodology. If using a scoring mechanism, apply a criticality score to each critical cyber infrastructure asset.
- □ Discuss and document what redundancies or backups are available to put in place for those services. For example, some services may be able to run manually or be relocated to a non-impacted location.

□ Rank the critical cyber infrastructure using the identified methodology or criticality score. Be sure to consider redundancies and back-ups as mitigating factors.

□ Use this information to establish priorities for applying limited resources and defining an order of response efforts.

Sample Critical Cyber Infrastructure Scoring Mechanism

This sample scoring mechanism provides an example approach for assessing cyber infrastructure criticality.

In this sample, the numbers in parentheses represent the associated score for each response. The total score is calculated after all questions are completed. Note: Infrastructure(s) with higher scores represent those that may be considered higher priorities.

When creating or utilizing a critical cyber infrastructure scoring mechanism, each jurisdictions define a rating system for assessing impact that is appropriate for its community to enable a consistent impact estimation throughout the asset prioritization process. Below are definitions for a potential rating system adapted from the National Institute of Standard and Technology (NIST) Standards for Security Categorization of Federal Information and Information Systems.[2]

Minor impact: Limited adverse effect that might: (i) cause a degradation in mission capability to an extent and duration that the jurisdiction is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minimal damage to the jurisdiction's assets; (iii) result in minimal financial loss; or (iv) result in minimal harm to individuals.

Moderate impact: Serious adverse effect that might: (i) cause a significant degradation in mission capability to an extent and duration that the jurisdiction is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to the jurisdiction's assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Severe impact: Catastrophic adverse effect that might: (i) cause a severe degradation of mission capability to an extent and duration that the is able to perform its primary functions, but the effectiveness of the functions is severely reduced; (ii) result in major damage to the jurisdiction's assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries

Complete disruption: Catastrophic adverse effect that causes a severe degradation or loss of mission capability to an extent and duration that the jurisdiction is not able to perform one or more of its primary functions.

[2] U.S. Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems, February 2004.

1. Estimate the level of impact the loss or impairment of this infrastructure would have on the jurisdiction’s ability to govern.

   □ No impact (0)

   □ Minor (1)

   □ Moderate (2)

   □ Severe (3)

   □ Complete disruption (4)

2. Estimate the level of impact the loss or impairment of this infrastructure would have on the jurisdiction’s emergency response capabilities.

   □ No impact (0)

   □ Minor (1)

   □ Moderate (2)

   □ Severe (3)

   □ Complete disruption (4)

3. Estimate the level of impact the loss or impairment of this infrastructure would have on the jurisdiction’s ability to provide medical care and public health services.

   □ No impact (0)

   □ Minor (1)

   □ Moderate (2)

   □ Severe (3)

   □ Complete disruption (4)

4. Estimate the level of impact the loss or impairment of this infrastructure would have on the jurisdiction’s ability to provide public safety.

   □ No impact (0)

   □ Minor (1)

   □ Moderate (2)

   □ Severe (3)

   □ Complete disruption (4)

5. Estimate the level of economic impact the loss or impairment of this infrastructure would have on the jurisdiction.

   □ No impact (0)

   □ Minor (1)

   □ Moderate (2)

   □ Severe (3)

   □ Complete disruption (4)

6. Estimate the level of impact the loss or impairment of this infrastructure would have on the jurisdiction's ability to provide basic essential services, such as water, electricity, or gas.

   □ No impact (0)

   □ Minor (1)

   □ Moderate (2)

   □ Severe (3)

   □ Complete disruption (4)

7. Would the loss or impairment of this infrastructure result in cascading disruption to other infrastructure or key resources?

   □ No (0)

   □ Yes (1)

8. Would knowledge of the loss or substantial impairment of this infrastructure undermine the public's morale or confidence in governmental and/or economic institutions?

   □ No (0)

   □ Yes (1)

9. Estimate the time for loss of this infrastructure before severe impact.

   □ Could be postponed or performed in another manner for 7 or more days. (1)

   □ Could be disrupted or unavailable for 1-7 days without significant consequence. (2)

   □ Must be restored within 24 hours to avoid severe consequences. (3)

   □ Must be restored within 12 hours to avoid severe consequences. (4)

Total Score: