Summary of the Cybersecurity Policy for CIP (4th Edition)

   - Promotion of activities for **reduction of Critical Infrastructure Services (CISs) outage risk** resulting from cyberattacks, natural disasters, etc. and **ensuring resilience** in order to **provide CISs safely and continuously**, based on **active involvement of top management** (Mission Assurance)
   - Essential services for organizing the Olympic and Paralympic games shall be secured.

2. Challenges
   - CI operators are **gradually coming to take on voluntary activities**, and still have some challenges on Check & Act in the PDCA cycle
   - Improve information sharing not only IT but also OT (Operational Technology) and **promote incident readiness**
   - Continue and improve **provision of information to the nation** through analysis and cooperation with various entities all over the world

3. Policy Priorities
   - **(1) Promotion of Leading Activities (Classification)**
     - Enforcing and improving the leading activities of some sectors (such as Electric power supply, Information & Communication and Financial services), which are highly depended upon by other CISs and cause a big impact on society in the case of outages
     - Encouraging other CI operators by expanding the leading activities
   - **(2) Enhancement of Information Sharing System toward the Olympic and Paralympic Games**
     - Considering introduction of the severity schema on CISs outages
     - Breaking the barrier of information sharing by diversifying the contact formation (Anonymization, sharing via the CEPTOAR* Secretariat, Cybersecurity related agencies)
     - Study of gathering cross-sectoral information into the cabinet secretariat
     *Capability for Engineering of Protection, Technical Operation, Analysis and Response
     - Development of information sharing system utilizing the hotline (Automation, Work saving, Expediting, Ensuring)
     - Clarification of the scope of information sharing and provision including the OT, IoT, etc.
     - Maintenance and improvement of CIP capability by improvement of exercises and penetration of the results
     - Expanding the protection scope as “protection as plane” including the supply chain
   - **(3) Promotion of Incident Readiness Based on Risk Management**
     - Dissemination of risk assessment by providing “the risk assessment guideline for mission assurance” and workshops
     - Promotion of incident readiness of CI operators by establishing BCPs and contingency plans
     - Enhancing the monitoring and review by providing the perspective of internal audit in risk management and incident readiness

4. Duration
   - The 4th Edition will cover until the end of the Olympic and Paralympic games, and will be revised even within the period as necessary.
Promoting CIP through public-private partnership

On the basis of the concept of mission assurance, in order to safely and continuously provide critical infrastructure services (CISs) and to avoid serious effects on the national life and socioeconomic activities from CISs outages resulting from cyber-attacks, natural disasters or other causes, all stakeholders should protect the critical infrastructures by reducing the occurrence of CISs outages as much as possible and by ensuring prompt recovery from outages.
Purpose of "critical infrastructure protection"

In order to **safely and continuously provide** critical infrastructure services (CISs) and to avoid serious effects on the national life and socioeconomic activities from **CISs outages resulting from cyberattacks, natural disasters or other causes**, all stakeholders should protect the critical infrastructures by **reducing** the risk of CISs outages as much as possible and by ensuring **prompt recovery** from outages.

"Basic principles"

**In the first place, critical infrastructure operators should implement cybersecurity measures on their own responsibility.**

On the basis of the concept of mission assurance for all CIs, a sense of security should be nurtured among the public through CI protection activities in cooperation between Government and the private sector.

- The critical infrastructure operators should respectively take measures and make effort for continuous improvement of those measures as entities providing services and bearing social responsibilities.
- **Government organizations** should **provide necessary support** for critical infrastructure operators' cybersecurity activities.
- Each critical infrastructure operator should **cooperate and coordinate with other stakeholders** due to the limit of each operator’s individual cybersecurity measures to address various threats.
Responsibility of stakeholders (critical infrastructure operators, government organizations, cybersecurity related agencies, etc.)

- All stakeholders should periodically check the progress of their own measures and policies as part of relevant efforts and **accurately recognize the current circumstances**, and **proactively determine the goals of relevant activities**. In addition, stakeholders should **enhance their cooperation with each other**, taking into account the status of other stakeholders' relevant activities.
- All stakeholders should understand the 5W1H (when, where, who, why, what and how) of responses to CISs outages depending on the scale thereof and should be able to calmly address signs or occurrence of any CISs outages. They should also be capable of cooperating with other stakeholders and **respond in a cooperative and concerted manner** in addition to **ensuring robust communication among various stakeholders** and taking proactive measures.

Responsibility of critical infrastructure operators’ executives and senior managers

- Recognize **their responsibility for ensuring cybersecurity** and exert their leadership in cybersecurity measures from the viewpoint of mission assurance
- With the awareness that their individual efforts also contribute to the development of society as a whole, take cybersecurity measures while **involving their supply chains (business partners, subsidiaries and affiliated companies, etc.)**
- Develop incident readiness even in normal times and **disclose information** on responses properly in the event of an incident from the perspective of **gaining trust and nurturing a sense of security among stakeholders**
- **Constantly secure management resources**, such as budgets, systems and personnel, necessary for the abovementioned measures and **devise risk-based allocation thereof**
Policy Group (1): Maintenance and Promotion of the Safety Principles

Look to continual improvement of the “guidelines" and “safety principles" under the PDCA cycle of security activities in order to maintain and strengthen the ability of critical infrastructure protection

* Safety principles: Generically refer to relevant laws, industry standards/guidelines, internal regulations (IR), etc.
* Guidelines: Contain items of measures that are most necessary from a cross-sectoral perspective, in order to contribute to preparation and revision of safety principles

Current Issues

- The PDCA cycle that allows CI operators to judge the necessity of review and improve independently is prevailing in the code of conduct of CI operators. However, the activities of “Check” and “Act" in the PDCA cycle are not established.

Activities during this Cybersecurity Policy term

1. Continual improvement of the guidelines for safety principles
   - Describing the details about the formation of cybersecurity culture and items and actions which top management who are responsible for carrying out the PDCA cycle must recognize.
   - Describing the necessity of preparation of incident readiness by establishment of BCP, contingency plans, etc. on the basis of the mission assurance.

2. Continual improvement of the safety principles
   - Promotion of improvement process of standards and guidelines which reflects the PDCA cycle.
   - Continual improvement of the institutional framework such as positioning the cybersecurity activities as safety regulation, embodiment of service maintenance level in relevant laws.

3. Promotion of the safety principles
   - Understanding the status of security measure through the annual questionnaire of CI operators, etc.
   - Utilizing the answer of questionnaire, supporting CI operators to be able to recognize issues of measures, solutions, etc.
Policy Group (2): Enhancement of Information Sharing System

To rapidly address each CI operator’s cybersecurity trends that change from day to day, further enhance information sharing between the public and private sectors, within a sector, and among sectors and/or outside sectors

Current Issues
- The understanding of the significance and necessity of information sharing is not sufficient in some CI operators.
- The lack of prompt and effective information sharing system in some CI operators.
- The understanding of information to be shared may not be sufficient.
- The dissemination and promotion of voluntary efforts by CI operators may not be sufficient.

Activities during this Cybersecurity Policy term

(1) Improvement of the information sharing system
- Adding new contact formation
- Preparation of the information sharing system for Olympic and Paralympic games.
- Positive cooperation with cybersecurity related agencies

(2) Further promotion of information sharing
- Consideration of introduction of the severity schema on CISs outages.
- Defining information to be shared
  - Including the information of OT, IoT, etc. in the scope of information sharing and providing.

(3) Further activation of private activities
- Further improvement of information sharing within the CEPTOAR or among CEPTOARs
- Spreading the activities such as ISAC doing leading activities

【Information sharing system Activities during this Cybersecurity Policy term】

Activities based on this Cybersecurity Policy
Policy Group (3): Enhancement of Incident Response Capability

Maintain and enhance the CIP capability through improvement of exercises and training which fit the actual state of response of CISs outages in operators and exercise needs.

Current Issues

- Planning and promotion of more effective and practical cross-sectoral exercises
- Spreading of participants in cross-sectoral exercises
- Spreading and promotion of lessons learned from cross-sectoral exercises fit for the roll of each stakeholder in service outage

Activities during this Cybersecurity Policy term

1. Continuous improvement of cross-sectoral exercises
   - Planning of exercises that fit the actual state of CI operators
     - Taking needs from CI operators in exercises
     - Maintenance of exercise scenarios reflecting the latest trends
     - Extending the scope of participants such as other operators except CI operators and those closely related to CI

2. Increasing participants for more spreading of lessons learned
   - Promotion for new participants
   - Mutual cooperation with other exercises / training
   - Planning exercises that are able to promote the understanding of top management
   - Return the know-how of exercises that contribute to holding the exercises independently (provision of a virtual exercise environment)

Summary of cross-sectoral exercises

- Planning exercises that are able to promote the understanding of top management
- Return the know-how of exercises

Activities based on this Cybersecurity Policy

- (1) Reporting situation to Government under public-private cooperation, obtaining aggregated information from Government
- (4) Releasing information to media, customers, consumers, etc.
- (5) Recording action on memo
- (3) Sharing information with related organizations
- (2) Sharing information with other sectors and within same sector
- Continuous improvement of cross-sectoral exercises
  - Planning of exercises that fit the actual state of CI operators
  - Promotion for new participants including operators except CI operators
  - Mutual cooperation with other exercises / training
  - Planning exercises that are able to promote the understanding of top management
  - Return the know-how of exercises

Maintain and Improve the CIP capability
Policy Group (4): Risk Management and Preparation of Incident Readiness

Promote risk management that CI operators implement and the preparation of incident readiness to achieve safe and continuous CI service provision

**Current Issues**
- Recognition of the importance of risk assessment is spreading, but the concept and ways to implement it have not spread sufficiently.
- Needs for preparation of incident readiness are growing in case of CISs outages, but specific directions, supporting measures, etc. are not shown.

**Activities during this Cybersecurity Policy term**

1. **Basic view of risk management**
   - Promotion of risk management
     - Dissemination of risk assessment
       - Promotion of implementation of risk assessment for Olympic and Paralympic games
       - Maintenance and dissemination of risk assessment guidelines based on the concept of mission assurance
     - Investigation and analysis of new risk sources and risks, etc.
       - Environment change studies
       - Interdependency analysis
   - Promotion of incident readiness
     - Arrangement of points in BCPs and contingency plans based on the concept of mission assurance
     - Establishment of organization responsible to share the incident information for the Olympic and Paralympic games
   - Promotion of risk communication and consultation
     - Provision of opportunities for information and opinion sharing among stakeholders, including internal stakeholders
   - Promotion of monitoring and review
     - Arrangement of audit perspective such as independent internal audit in CI operators.

3. **Establishment of process of reflection to and from other activities**

**Activities based on this Cybersecurity Policy**

- **Risk Assessment (Identification・Analysis・Evaluation)**
- **Risk Treatment (Promotion of incident readiness)**
- **Monitoring and review**
- **Dissemination of risk assessment**
  - Promotion of implementation of risk assessment for Olympic and Paralympic games
  - Maintenance and dissemination of risk assessment guidelines
- **Investigation and analysis of new risk sources and risks, etc.**
  - Environment change studies
  - Interdependency analysis

**Promotions**
- Promotion of incident readiness
- Promotion of risk communication and consultation
- Promotion of monitoring and review
- Arrangement of points in BCPs and contingency plans
- Providing opportunities
- Arrangement of audit perspective

**Establishment of organization responsible to share the incident information for the Olympic and Paralympic games**
Policy Group (5): Enhancement of the Basis for CIP

Enhance common foundation activities that support the whole of this Cybersecurity Policy such as review of the protection scope of CI, public relations, international cooperation, appeal to top management and developing human resources, etc.

**Current Issues**
- “Protection as plane” for response to environment change
- Further promoting of public relations
- Improvement of international cybersecurity measure level
- Improvement of mindset of top management on cybersecurity
- Further quantitative and qualitative enhancing of human resources

**Activities during this Cybersecurity Policy term**

1. Review of the protection scope of CI
   - Activities towards “protection as plane” and from the perspective of securing national security

2. Promotion of public relations activities
   - Positive sending of frameworks of this Cybersecurity Policy, activities, etc. for the nation

3. Promotion of international cooperation
   - Positive contribution to Improvement of international cybersecurity measure level

4. Appeal to top management
   - Appeal for improvement of awareness of top management on cybersecurity

5. Promotion of the development of human resources
   - Promotion of development of bridge human resources, building of cross-sectoral system, exercises and qualification of cybersecurity, etc.

**Review of the protection scope of CI**

**Protection as dot:** Protect 14 islands
- Expand the edges: Protect 14 offshore territories
- Further expansion: Protect the Exclusive Economic Zone

**Protection as plane:** Protect the globe

- Public relations activities: Promotion via Web, lecture, etc.
- International cooperation: Cooperation of bilateral, inter-regional, and multilateral frameworks,
- Appeal to top management: Developing human resources
- Promoting the activities based on the “Cybersecurity Experts Development Program”
"Critical Infrastructure Operator Measure Examples" and "Government Activities"

Maintenance and promotion of the safety principles
Continual improvement of the safety principles (Secretariat/responsible ministries for critical infrastructure)
Survey on activities under safety principles (Cabinet Secretariat)

Risk management and preparation of incident readiness
Risk communication and consultation (Cabinet Secretariat/responsible ministries for critical infrastructure)

Information sharing
Information sharing between public-private stakeholders (Cabinet Secretariat/responsible ministries for critical infrastructure)

Incident response
Cross-sectoral exercises (Cabinet Secretariat/responsible ministries for critical infrastructure)
CEPTDoAR communication training (Cabinet Secretariat/responsible ministries for critical infrastructure)
Training by responsible ministries for critical infrastructure (Responsible ministries for critical infrastructure)

Enhancement of basis for critical infrastructure protection
Review of the protection scope / Public relations / International cooperation / Promotion of security by design / Appeal to top management / Promotion of the developing human resources / maintenance of regulations (Cabinet Secretariat/responsible ministries for critical infrastructure)
CEPTOAR and CEPTOAR Council


- Organization responsible for information sharing and analysis functions and relevant functions for critical infrastructure operators.
- For proactive prevention of CISs outages as well as prevention of the spread of damage, prompt recovery, and prevention of recurrence in the case of CISs outages, CEPTOARs appropriately provide information provided by the Government, etc. to critical infrastructure operators and share information with stakeholders. CEPTOARs hereby aim at activities that contribute to the improvement of the service maintenance and recovery capability of each critical infrastructure operator.

CEPTOAR council

- This is a council consisting of representatives from CEPTOARs developed in each critical infrastructure sector. It shares information between CEPTOARs. It is an independent meeting structure that is not positioned under any other organizations including government organizations.
- The council was founded on February 26, 2009, with the purpose of promoting cross-sectoral information sharing.
# The list of CEPTOARs (14 sectors, 19 CEPTOARs)

## CI Sectors

<table>
<thead>
<tr>
<th>Services</th>
<th>Financial</th>
<th>Aviation</th>
<th>Airport</th>
<th>Railway</th>
<th>Electric power supply</th>
<th>Gas supply</th>
<th>Government and administrative</th>
<th>Medical</th>
<th>Water</th>
<th>Logistics</th>
<th>Chemical</th>
<th>Credit card</th>
<th>Petroleum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>Information and communication</td>
<td>Financial</td>
<td>Aviation</td>
<td>Airport</td>
<td>Railway</td>
<td>Electric power supply</td>
<td>Gas supply</td>
<td>Government and administrative</td>
<td>Medical</td>
<td>Water</td>
<td>Logistics</td>
<td>Chemical</td>
<td>Credit card</td>
</tr>
<tr>
<td>Services</td>
<td>Electrical communication</td>
<td>Banking</td>
<td>Securities</td>
<td>Life insurance</td>
<td>General insurance</td>
<td>Aviation</td>
<td>Airport</td>
<td>Railway</td>
<td>Electric power supply</td>
<td>Gas supply</td>
<td>Government and administrative</td>
<td>Medical</td>
<td>Water</td>
</tr>
<tr>
<td>Services</td>
<td>Broadcasting</td>
<td>General aviation</td>
<td>Electric power supply</td>
<td>Gas supply</td>
<td>Government and administrative</td>
<td>Medical</td>
<td>Water</td>
<td>Logistics</td>
<td>Chemical</td>
<td>Credit card</td>
<td>Petroleum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td>T-Cable TV</td>
<td>Financial service CEPTOAR</td>
<td>Aviation services CEPTOAR</td>
<td>Gas supply services CEPTOAR</td>
<td>Gas supply services CEPTOAR</td>
<td>Local government</td>
<td>Medical services CEPTOAR</td>
<td>Water supply CEPTOAR</td>
<td>Logistics</td>
<td>Chemical industries CEPTOAR</td>
<td>Credit card services CEPTOAR</td>
<td>Petroleum industries CEPTOAR</td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td>Broadcasting CEPTOAR</td>
<td>Banking services etc. CEPTOAR</td>
<td>Life insurance services CEPTOAR</td>
<td>General insurance services CEPTOAR</td>
<td>Aviation services CEPTOAR</td>
<td>Airport services CEPTOAR</td>
<td>Railway services CEPTOAR</td>
<td>Electric power supply services CEPTOAR</td>
<td>Medical services CEPTOAR</td>
<td>Water supply CEPTOAR</td>
<td>Logistics services CEPTOAR</td>
<td>Chemical industries CEPTOAR</td>
<td>Credit card services CEPTOAR</td>
</tr>
<tr>
<td>Services</td>
<td>Financial service CEPTOAR Liaison Council</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Member

<table>
<thead>
<tr>
<th>Member</th>
<th>Information and communication</th>
<th>Financial</th>
<th>Aviation</th>
<th>Airport</th>
<th>Railway</th>
<th>Electric power supply</th>
<th>Gas supply</th>
<th>Government and administrative</th>
<th>Medical</th>
<th>Water</th>
<th>Logistics</th>
<th>Chemical</th>
<th>Credit card</th>
<th>Petroleum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>CI sectors</td>
<td>23 companies</td>
<td>1,411 companies</td>
<td>5 companies</td>
<td>14 companies</td>
<td>14 companies</td>
<td>10 companies</td>
<td>47 states</td>
<td>1,741 local governments</td>
<td>1 group</td>
<td>9 organizations</td>
<td>8 business units</td>
<td>17 companies</td>
<td>13 companies</td>
</tr>
<tr>
<td>Member</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Sharing Scope of info from NISC

<table>
<thead>
<tr>
<th>Sharing Scope of info from NISC (Except member)</th>
<th>Information and communication</th>
<th>Financial</th>
<th>Aviation</th>
<th>Airport</th>
<th>Railway</th>
<th>Electric power supply</th>
<th>Gas supply</th>
<th>Government and administrative</th>
<th>Medical</th>
<th>Water</th>
<th>Logistics</th>
<th>Chemical</th>
<th>Credit card</th>
<th>Petroleum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharing Scope of info from NISC (Except member)</td>
<td>CI sectors</td>
<td>23 companies</td>
<td>1,411 companies</td>
<td>5 companies</td>
<td>14 companies</td>
<td>14 companies</td>
<td>10 companies</td>
<td>47 states</td>
<td>1,741 local governments</td>
<td>1 group</td>
<td>9 organizations</td>
<td>8 business units</td>
<td>17 companies</td>
<td>13 companies</td>
</tr>
<tr>
<td>Sharing Scope of info from NISC (Except member)</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing Scope of info from NISC (Except member)</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing Scope of info from NISC (Except member)</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing Scope of info from NISC (Except member)</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing Scope of info from NISC (Except member)</td>
<td>and communiti es</td>
<td>1 community</td>
<td>197 companies and community</td>
<td>7 organizations</td>
<td>41 companies</td>
<td>1 community</td>
<td>3 companies and communities</td>
<td>170 companies and communities</td>
<td>381 companies and institutions</td>
<td>Spreading to 1341 business units as needed</td>
<td>Other (Nuclear material related office, building automation association, cyber defense Council, college)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As of July 25, 2018
Summary

Considering that the affected area and incident response activities are different depending on the severity of Critical Infrastructure Services (CISs) outages and the importance of related information, aiming at enhancement of recognition sharing among stakeholders and quick decision making on incident response, Severity schema on CISs outages should be established and discussed in detail.

Purpose

1. To promote common understanding among stakeholders about the incident, objectivity and international coordination
2. To provide a standard for decision making concerning government activities on incident response
3. To provide a standard for structure and method of information sharing

Severity Schema on CISs Outages (draft version)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 5 Emergency</td>
<td>poses an imminent threat to wide-scale critical infrastructure services</td>
</tr>
<tr>
<td>Level 4 Severe</td>
<td>likely to result in a significant impact on critical infrastructure services</td>
</tr>
<tr>
<td>Level 3 High</td>
<td>likely to result in a demonstrable impact on critical infrastructure services</td>
</tr>
<tr>
<td>Level 2 Medium</td>
<td>may affect critical infrastructure services</td>
</tr>
<tr>
<td>Level 1 Low</td>
<td>unlikely to affect critical infrastructure services</td>
</tr>
</tbody>
</table>

(Source: The Cybersecurity Policy for CIP 4th edition)

Table 1: Severity Schema on CISs Outages (draft)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Impact on People &amp; Society</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 5 Emergency</td>
<td>poses an imminent significant threat to wide-range national life, etc.</td>
</tr>
<tr>
<td>Level 4 Severe</td>
<td>likely to result in a significant impact on national life, etc.</td>
</tr>
<tr>
<td>Level 3 High</td>
<td>likely to result in a demonstrable impact on national life, etc.</td>
</tr>
<tr>
<td>Level 2 Medium</td>
<td>may affect national life, etc.</td>
</tr>
<tr>
<td>Level 1 Low</td>
<td>unlikely to affect national life, etc.</td>
</tr>
<tr>
<td>Level 0 Baseline</td>
<td>will not affect national life, etc.</td>
</tr>
</tbody>
</table>

Table 2: Draft version for discussion