



National Security Agency/Central Security Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Contingency Planning Capability

Version 1.1.1

The Contingency Planning Capability focuses on Information System Contingency Planning, which refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption (National Institute of Standards and Technology [NIST] Special Publication [SP] 800-34). The purpose of Information Systems Contingency Planning is to ensure the business and mission functions of an Organization under all circumstances.

07/30/2012



# CGS Contingency Planning Capability



Version 1.1.1

## Table of Contents

1	Revisions .....	2
2	Capability Definition .....	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions.....	6
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations .....	6
7	Capability Interrelationships.....	8
7.1	Required Interrelationships .....	8
7.2	Core Interrelationships .....	10
7.3	Supporting Interrelationships.....	10
8	Security Controls .....	10
9	Directives, Policies, and Standards .....	17
10	Cost Considerations .....	23
11	Guidance Statements.....	23



# CGS Contingency Planning Capability



Version 1.1.1

## 1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1



# CGS Contingency Planning Capability



Version 1.1.1

## 2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Contingency Planning establishes policy, procedures, and technical measures designed to maintain or restore business operations. This includes computer operations (possibly at an alternate location) in the event of emergencies, system failures, or disasters. Contingency Planning occurs under all circumstances, including major disasters and events.

The Contingency Planning Capability focuses on Information System Contingency Planning, which refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption (National Institute of Standards and Technology [NIST] Special Publication [SP] 800-34). The purpose of Information Systems Contingency Planning is to ensure the business and mission functions of an Organization under all circumstances.

## 3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Contingency Planning Capability is responsible for maintaining the operations of critical systems, supports mission-essential functions, and prevents significant loss from system or resource disruption. In addition, the Contingency Planning Capability covers the technical, personnel, physical, and environmental aspects of the Enterprise in relation to information systems.

The Contingency Planning Capability requires the development of contingency and continuity planning programs to meet a variety of requirements. Enterprises shall not develop these programs independent of one another, and plans shall map to higher level national and federal policies (see the Directives, Policies, and Standards section).



# CGS Contingency Planning Capability



Version 1.1.1

Information System Contingency Planning shall always be done to meet requirements outlined in applicable standards. Contributors to the Contingency Plan shall be knowledgeable in standards and policies, and the team shall include subject matter experts. Enterprises shall understand dependencies on other Contingency Plans and integrate their contingency and continuity planning activities in a single, efficient, and focused effort to better prepare for undesirable events.

To develop an Information System Contingency Plan, business and mission priorities shall be developed to define the business impact analysis. There shall be an understanding of mission objectives and how systems relate to those missions. This will help in determining the system availability requirements and dependencies that are needed to make a decision regarding specific contingency solutions. The Contingency Planning Capability shall leverage the Understand Mission Flows Capability to provide the mission flow and priorities, and the Utilization and Performance Management Capability to understand recovery objectives and minimize downtime. This information shall be leveraged during analysis and definition of the Contingency Plan. It will be used to determine the information systems and availability requirements needed to support continuity of operations.

The Contingency Planning Capability shall address Operations Contingency planning. There shall be a relevant Contingency Plan documented for every realistically foreseeable event that could affect the Enterprise. Planning shall be agile and proactive to take into account any event or disaster that may occur to ensure the ability to continue business. The Information System Contingency Plan shall designate local and distant alternate facilities, and planning shall be done in such a way to ensure the Enterprise operates in the manner it should before, during, and after a major catastrophe.

Information System Contingency Plans shall identify critical resources such as services and systems that support mission functions. Plans shall map across different areas of responsibility if there are interdependencies. The plan shall define what level of disruption is allowable for those resources that can withstand a disruption and within what timeframe they have to be restored. For low-critical functions, there shall be some degree of reconstitution of data, as provided in the Data Protection Capability.

As a part of the Contingency Planning Capability, a process shall be defined to assess incidents and decide which Contingency Plan shall be implemented. The plan shall establish policy for allowable response times and policy covering mission availability



# CGS Contingency Planning Capability



Version 1.1.1

fluctuations that may occur if a mission system has to be switched over to a contingency system. To support the restoration of disrupted services, the Contingency Planning Capability shall include approaches such as restoring information systems through the use of alternate equipment, potentially performing business processes through manual means, recovering information systems operations at an alternate location, and implementing appropriate Contingency Planning controls. The approach used shall be dependent on the allowable length of time a service is to be unavailable (e.g., short term or long term), and the criticality of the service that is disrupted.

Full-scale emergency response exercises shall be planned and conducted to validate that the Contingency Plan meets mission assurance requirements. Full-scale exercises shall be approved by senior management with concurrence from a mission analysis group based on criticality and mission impact. Decision-makers shall determine, based on these factors, whether real-world testing is required. In cases where it is not required, the type and scope of an exercise shall be defined. Exercises shall be conducted annually.

The Contingency Planning Capability shall be continuously monitored to determine when new Information System Contingency Planning needs arise. Defined Contingency Plans shall be reevaluated and updated annually, as necessary. However, the reevaluation may also be triggered based on changes identified from the Risk Analysis, Understand Mission Flow, and Utilization and Performance Management Capabilities. The Contingency Planning Capability includes the ability to provide flexible Contingency Planning that is based on risk (as provided from the Risk Analysis Capability) and mission impact (as provided from the Understand Mission Flows Capability). The Contingency Planning approach shall be responsive to operational changes and tie together information such as mission criticality, resource requirements, and information received from other Capabilities to reassess Contingency Planning in a timely manner.

Information System Contingency Plans shall be centrally managed. The Contingency Planning Capability shall provide a process for distributing and notifying interested parties of new or updated Contingency Plans.

The Contingency Planning Capability shall leverage the IA Training and IA Awareness Capabilities to ensure that all users receive and understand their roles and responsibilities and the purpose of the Contingency Plans. Any revisions to the Contingency Plan shall be communicated to relevant users through training and awareness activities.



# CGS Contingency Planning Capability



Version 1.1.1

Information System Contingency Plans shall be developed in coordination with other Enterprises to maintain Enterprise interoperability and cross-Enterprise mission flow. Communication across Enterprises shall occur if there is a disruption that may affect others, to help ensure they are prepared.

## 4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Mission and business objectives and priorities are clearly understood.
2. System availability requirements are clearly known.
3. Incident response processes are defined and implemented.
4. System interdependencies are known.
5. Mission impact may change over time.
6. Continuity of Operations has been defined and system requirements are known.
7. System lifecycle processes are synchronized with the Contingency Plan.

## 5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability ensures information systems support requirements for mission-essential functions before, during, and following any circumstance (e.g., a major catastrophic disaster).
2. The Capability ensures all functions will be reconstituted after an event.
3. The Capability includes how the contingency plan will be executed in the context of an overall information technology (IT) disaster recovery plan.
4. The Capability ensures information systems meet or exceed the requirements defined in NIST SP 800-34.

## 6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an



# CGS Contingency Planning Capability



Version 1.1.1

Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

Contingency Planning directly supports an Organization's goal of continued operations and establishes a set of plans to maintain mission operations in the event of an attack, outage, or other form of service disruption. Information System Contingency Planning addresses how to keep an Organization's critical functions operating in the event of disruptions, both large and small.

Each Organization will ensure its Contingency Plans are based on information such as mission criticality, resource requirements, recovery objectives, and maximum downtime, which is provided by other Capabilities (e.g., Understand Mission Flow and Utilization and Performance Management). Risk Analysis information will also be used to help determine an optimal strategy.

The Organization will ensure the Information System Contingency Plan identifies mission and business functions and ensure appropriate priorities are set and approved by senior management, so that in the event of a disaster, certain functions are not performed. An Organization will identify the resources that support critical functions. The analysis of needed resources will be conducted by subject matter experts who understand how the function is performed and the interdependencies among various resources. This allows an Organization to assign priorities to resources because not all elements are crucial to critical functions. There may be instances in which the identification of resources will cross areas of responsibility, and common resources will be used such as people, processing capability, data and applications, and physical infrastructure. Organizations will ensure Contingency Plans map across all areas. In addition, each Organization will identify operational requirements for a resource (e.g., whether the resource is needed constantly or only on a periodic basis), and the effect on the mission or business of the continued unavailability of the resource.

When developing the Contingency Plan, each Organization will document the initial actions that will be taken to minimize damage, plan the steps that will be taken to continue support for critical mission and business functions without disruption, and determine what will be required to ensure all functions will be reconstituted after an event. The Organization will activate different Contingency Plans based on the severity and nature of an event. For example, a system outage will be handled differently if it is due to an unexpected utilities outage, a digital intrusion, or a physical attack. The Organization will ensure subject matter experts and security engineers who understand



# CGS Contingency Planning Capability



Version 1.1.1

the mission, data, systems, and Enterprise view are included and the appropriate decision authority approves the plan.

Organizations will ensure appropriate systems are in place and document procedures. Each Organization will use techniques such as load balancing and system redundancy to maintain system availability requirements. Organizations will also provide a redundant environment and a geographically separate backup site for Enterprise systems.

Organizations will ensure Information System Contingency Plans are stored in a centralized repository. Each Organization will define a process for distributing notification of new Contingency Plans to interested parties and ensure distribution occurs in a timely manner. An Organization will ensure all new users receive training on any relevant Information System Contingency Plans, and all existing users will be able to demonstrate a requisite level of understanding of these plans. Whenever there is a revision to a Contingency Plan, all relevant users will be provided access to the revised plan and a briefing on the changes.

An Organization will develop exercises to ensure that the plan is defined properly and will work. Scenarios will be used to figure out what courses of action will be taken. The Organization will conduct exercises regularly. Feedback from these exercises will be incorporated into Contingency Plan revisions. Exercises will be used to test both technology systems and user readiness. Each Organization will test and revise the Contingency Plan periodically based on lessons learned, mission impact, and changes to resources used to support critical functions. The extent and frequency of testing will vary between Organizations and among systems.

## 7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

### 7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.



# CGS Contingency Planning Capability



Version 1.1.1

- Network Mapping-The Contingency Planning Capability relies on the Network Mapping Capability for information used to understand the Enterprise environment, inform its processes, and formulate the details for the contingency plans.
- Network Boundary and Interfaces-The Contingency Planning Capability relies on the Network Boundary and Interfaces Capability for information used to understand the Enterprise environment, inform its processes, and formulate the details for the contingency plans.
- Utilization and Performance Management-The Contingency Planning Capability relies on the Utilization and Performance Management Capability for information used to understand the Enterprise environment, inform its processes, and formulate the details for the contingency plans.
- Understand Mission Flows-The Contingency Planning Capability relies on the Understand Mission Flow Capability for information used to understand the Enterprise environment, inform its processes, and formulate the details for the contingency plans.
- Understand Data Flows-The Contingency Planning Capability relies on the Understand Data Flows Capability for information used to understand the Enterprise environment, inform its processes, and formulate the details for the contingency plans.
- Hardware Device Inventory-The Contingency Planning Capability relies on the Hardware Device Inventory Capability for information used to understand the Enterprise environment, inform its processes, and formulate the details for the contingency plans.
- Software Inventory-The Contingency Planning Capability relies on the Software Inventory Capability for information used to understand the Enterprise environment, inform its processes, and formulate the details for the contingency plans.
- Understand the Physical Environment-The Contingency Planning Capability relies on the Understand the Physical Environment Capability for information used to understand the Enterprise environment, inform its processes, and formulate the details for the contingency plans.
- System Protection-The Contingency Planning Capability relies on the System Protection Capability to provide protection requirements that are used when defining contingency plans and procedures.
- Risk Analysis-The Contingency Planning Capability relies on the Risk Analysis for information used to make adjustments to its strategy as the Enterprise risk posture changes over time.



# CGS Contingency Planning Capability



Version 1.1.1

- Risk Monitoring-The Contingency Planning Capability relies on the Risk Monitoring Capability for information used to make adjustments to its strategy as the Enterprise risk posture changes over time.

## 7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management-The Contingency Planning Capability has a return-on-investment status that includes IA aspects provided to the Portfolio Management Capability by the Contingency Planning Capability.
- IA Policies, Procedures, and Standards-The Contingency Planning Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness-The Contingency Planning Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training-The Contingency Planning Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities-The Contingency Planning Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

## 7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- None.

## 8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information</i>	



# CGS Contingency Planning Capability



Version 1.1.1

<i>Systems and Organizations</i>	
<b>CP-2 CONTINGENCY PLAN</b>	<p>Control: The organization:</p> <ul style="list-style-type: none"> <li>a. Develops a contingency plan for the information system that: <ul style="list-style-type: none"> <li>- Identifies essential missions and business functions and associated contingency requirements;</li> <li>- Provides recovery objectives, restoration priorities, and metrics;</li> <li>- Addresses contingency roles, responsibilities, assigned individuals with contact information;</li> <li>- Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;</li> <li>- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and</li> <li>- Is reviewed and approved by designated officials within the organization;</li> </ul> </li> <li>b. Distributes copies of the contingency plan to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements];</li> <li>c. Coordinates contingency planning activities with incident handling activities;</li> <li>d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];</li> <li>e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and</li> <li>f. Communicates contingency plan changes to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements].</li> </ul> <p>Enhancement/s:</p> <ul style="list-style-type: none"> <li>(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.</li> <li>(2) The organization conducts capacity planning so that</li> </ul>



# CGS Contingency Planning Capability



Version 1.1.1

	<p>necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.</p> <p>(3) The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.</p> <p>(4) The organization plans for the full resumption of missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.</p> <p>(5) The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.</p> <p>(6) The organization provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.</p>
<p><b>CP-4 CONTINGENCY PLAN TESTING AND EXERCISES</b></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> <li>a. Tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and</li> <li>b. Reviews the contingency plan test/exercise results and initiates corrective actions.</li> </ul> <p>Enhancement/s:</p> <ul style="list-style-type: none"> <li>(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.</li> <li>(2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.</li> <li>(3) The organization employs automated mechanisms to more</li> </ul>



# CGS Contingency Planning Capability



Version 1.1.1

	<p>thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.</p> <p>(4) The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.</p>
<p><b>CP-6 ALTERNATE STORAGE SITE</b></p>	<p>Control: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.</p> <p>Enhancement/s:</p> <p>(1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.</p> <p>(2) The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.</p> <p>(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.</p>
<p><b>CP-7 ALTERNATE PROCESSING SITE</b></p>	<p>Control: The organization:</p> <p>a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period consistent with recovery time objectives] when the primary processing capabilities are unavailable; and</p> <p>b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.</p> <p>Enhancements:</p> <p>(1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.</p> <p>(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide</p>



# CGS Contingency Planning Capability



Version 1.1.1

	<p>disruption or disaster and outlines explicit mitigation actions.</p> <p>(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.</p> <p>(4) The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.</p> <p>(5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.</p>
<p>CP-8 <i>TELECOMMUNICATIONS SERVICES</i></p>	<p>Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.</p> <p>Enhancement/s:</p> <p>(1) The organization:</p> <p>(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.</p> <p>(2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.</p> <p>(3) The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.</p> <p>(4) The organization requires primary and alternate telecommunications service providers to have contingency plans.</p>
<p>CP-9 <i>INFORMATION SYSTEM BACKUP</i></p>	<p>Control: The organization:</p> <p>a. Conducts backups of user-level information contained in the</p>



# CGS Contingency Planning Capability



Version 1.1.1

	<p>information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];</p> <p>b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];</p> <p>c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and</p> <p>d. Protects the confidentiality and integrity of backup information at the storage location.</p> <p>Enhancement/s:</p> <p>(1) The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.</p> <p>(2) The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.</p> <p>(3) The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.</p> <p>(5) The organization transfers information system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives].</p> <p>(6) The organization accomplishes information system backup by maintaining a redundant secondary system, not collocated, that can be activated without loss of information or disruption to the operation.</p>
<p>CP-10  <i>INFORMATION SYSTEM RECOVERY AND</i></p>	<p>Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.</p> <p>Enhancement/s:</p>



# CGS Contingency Planning Capability



Version 1.1.1

<p><i>RECONSTITUTION</i></p>	<p>(1) [Withdrawn: Incorporated into CP-4].</p> <p>(2) The information system implements transaction recovery for systems that are transaction-based.</p> <p>(3) The organization provides compensating security controls for [Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state].</p> <p>(4) The organization provides the capability to reimage information system components within [Assignment: organization-defined restoration time-periods] from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.</p> <p>(5) The organization provides [Selection: real-time; near-real-time] [Assignment: organization-defined failover capability for the information system].</p> <p>(6) The organization protects backup and restoration hardware, firmware, and software.</p>
<p><i>PE-17 ALTERNATE WORK SITE</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> <li>a. Employs [Assignment: organization-defined management, operational, and technical information system security controls] at alternate work sites;</li> <li>b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and</li> <li>c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.</li> </ul> <p>Enhancement/s: None Specified.</p>
<p><i>PM-8 CRITICAL INFRASTRUCTURE PLAN</i></p>	<p>Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.</p> <p>Enhancement/s: None Specified</p>
<p><i>SI-13 PREDICTABLE FAILURE PREVENTION</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> <li>a. Protects the information system from harm by considering mean time to failure for [Assignment: organization-defined list of information system components] in specific environments of operation; and</li> <li>b. Provides substitute information system components, when needed and a mechanism to exchange active and standby roles of the components.</li> </ul>



# CGS Contingency Planning Capability



Version 1.1.1

	<p>Enhancement/s:</p> <p>(1) The organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.</p> <p>(2) The organization does not allow a process to execute without supervision for more than [Assignment: organization-defined time period].</p> <p>(3) The organization manually initiates a transfer between active and standby information system components at least once per [Assignment: organization-defined frequency] if the mean time to failure exceeds [Assignment: organization-defined time period].</p> <p>(4) The organization, if an information system component failure is detected:</p> <p>(a) Ensures that the standby information system component successfully and transparently assumes its role within [Assignment: organization-defined time period]; and</p> <p>(b) [Selection (one or more): activates [Assignment: organization-defined alarm]; automatically shuts down the information system].</p>
--	---

## 9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

### Contingency Planning Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 503 IC Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008, Unclassified	Summary: Contingency Planning and Contingency Plan Evaluation are a part of certification and accreditation.



# CGS Contingency Planning Capability



Version 1.1.1

IC CIO Information Assurance-System Security Plan Template, 2008	Summary: A Contingency Plan is required by the Intelligence Community (IC) Chief Information Officer (CIO) in all System Security Plans and references provided in the plan template.
Intelligence Community Information Assurance Architecture, Version 1.1 (final draft), 30 September 2010, Classified	Summary: The document describes the IC Information Assurance (IA) Framework of the IC IA Architecture IA Framework.
<b>Comprehensive National Cybersecurity Initiative (CNCI)</b>	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
<b>Department of Defense (DoD)</b>	
DoDD 3020.26, Department of Defense Continuity Programs, 9 January 2009, Unclassified	Summary: This directive: 1.1. Reissues reference (a) and changes its title. 1.2. Establishes the Defense Continuity Program (DCP) and the Defense Continuity Executive Steering Group (hereafter referred to as the "Continuity ESG"). 1.3. Revises continuity policies and assigns responsibilities for developing and maintaining the DCP to enhance the Department of Defense (DoD) readiness posture. 1.4. Authorizes publication of additional DoD issuances relating to the DCP and the Defense Continuity Security Classification Guide.
DoDD 5144.1 Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, 2 May 2005, Unclassified	Summary: This directive assigns responsibility to the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)) DoD CIO to maintain a consolidated inventory of DoD mission-critical and mission-essential information systems... and to develop and maintain Contingency Plans for responding to a disruption in the operation of those information systems.
DoDI 8510.01, DoD	Summary: This instruction established policy that all DoD



# CGS Contingency Planning Capability



Version 1.1.1

Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007, Unclassified	information systems shall be certified and accredited. Contingency Plans are a requirement of the certification and accreditation process.
DoDD O-8530.1 Computer Network Defense (CND), 8 January 2001, Classified	See CGS Classified Annex
CJCSI 6510.01E Information Assurance (IA) and Computer Network Defense (CND), 12 August 2008, Unclassified	Summary: This instruction assigns responsibilities to all DoD elements to develop, maintain, and test their information technology (IT) Contingency Plans. It points to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 for assistance in IT Contingency Planning.
<b>Committee for National Security Systems (CNSS)</b>	
CNSSI 1253 Version 1, Security Categorization for control selection for National Security Systems, October 2009, Unclassified	Summary: This policy mandates guidance, baselines, and parameters for categorization of systems and the selection and application of security controls for National Security Systems. This is necessary to apply NIST SP 800-53 guidance for National Security Systems.
NTISSI 1000 National Information Assurance Certification and Accreditation Process (NIACAP), April 2000, Unclassified	Summary: This instruction identifies the requirement that information systems have Contingency Plans and addresses their maintenance and evaluation. In addition, it requires they be tested periodically.
<b>Other Federal (OMB, NIST, ...)</b>	
Nothing found	
<b>Executive Branch (EO, PD, NSD, HSPD, ...)</b>	
HSD Federal Continuity Directive 1 (FCD1), Federal Executive Branch National Continuity	Summary: This directive provides direction to the federal executive branch for developing continuity plans and programs. Continuity planning facilitates the performance of executive branch essential functions during all-hazards



# CGS Contingency Planning Capability



Version 1.1.1

<p>Program and Requirements, February 2008, Unclassified</p>	<p>emergencies or other situations that may disrupt normal operations.</p>
<p>HSD Federal Continuity Directive 2 (FCD2), Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process , February 2008, Unclassified</p>	<p>Summary: This directive implements the requirements of FCD 1, Annex C. It provides guidance and direction to federal executive branch departments and agencies for identification of their Mission-essential Functions (MEFs) and potential Primary Mission-essential Functions (PMEFs).</p>
<p>Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection, 17 December 2003, Unclassified</p>	<p>Summary: This policy identifies the requirement that Information Systems Contingency Planning needs to address Critical infrastructure requirements required for the continuity of MEFs.</p>
<p>Homeland Security Presidential Directive 51/ National Security Presidential Directive 20, National Continuity Policy, 9 May 2007, Unclassified</p>	<p>Summary: This policy establishes “National Essential Functions,” prescribes continuity requirements for all executive departments and agencies, and provides guidance for state, local, territorial, and tribal governments, and private sector Organizations. This guidance is to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.</p>
<p>National Communications System (NCS) Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, 25 July 2007, Unclassified</p>	<p>Summary: This directive establishes policy, explains legal and regulatory basis, assigns responsibilities, and prescribes minimum requirements for continuity communications capabilities.</p>
<p>National Continuity Policy</p>	<p>Summary: This policy builds on the National Continuity</p>



# CGS Contingency Planning Capability



Version 1.1.1

Implementation Plan (NCPIP), September 2007, Unclassified	Policy and provides guidance to executive departments and agencies on appropriately identifying and carrying out their PMEFs that support the eight National Essential Functions-the most critical functions necessary to lead and sustain the nation during a catastrophic emergency. Information Systems Contingency Planning must support the requirements of the National Continuity Policy Implementation Plan (NCPIP).
NCPIP attachment B, September 2007, Unclassified	Summary: This document presents Essential Functions and the Interagency Board Process. Attachment to NCPIP.
NCPIP attachment C, September 2007, Unclassified	Summary: This document presents the Initial Requirements. Attachment to NCPIP.
Title 36, Code of Federal Regulations, Section 1236, Management of Vital Records, 16 May 2001, Unclassified	Summary: This policy identifies the requirement that information systems data backup and recovery must support vital records management requirements for Federal Continuity Directive 1 (FCD1).
<b>Legislative</b>	
Federal Information Security Management Act (FISMA) (P.L. 107-347-Title III), December 2002, Unclassified	Summary: This legislation requires Information Systems Contingency Planning to support the continuity of operations for the Organization's mission and business functions under any condition.

## Contingency Planning Standards

Title, Date, Status	Excerpt / Summary
<b>Intelligence Community (IC)</b>	
Nothing found	
<b>Comprehensive National Cybersecurity Initiative (CNCI)</b>	
Nothing found	
<b>Department of Defense (DoD)</b>	



# CGS Contingency Planning Capability



Version 1.1.1

Nothing found	
<b>Committee for National Security Systems (CNSS)</b>	
Nothing found	
<b>Other Federal (OMB, NIST, ...)</b>	
NIST SP 800-34, Rev 1, Contingency Planning Guide for Federal Information Systems, May 2010, Unclassified	Summary: This special publication (SP) provides guidance for Information System Contingency Planning to ensure it supports continuity of operations as mandated in HSPD51/NSPD20, FCD1, and NCS Directive 3-10.
NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010, Unclassified	Summary: This SP requires Information System Contingency Planning as part of the security plan, risk management, and mitigation process.
NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011, Unclassified	Summary: This SP requires Information System Contingency Planning as part of the security plan, risk management, and mitigation process.
<b>Executive Branch (EO, PD, NSD, HSPD, ...)</b>	
Nothing found	
<b>Legislative</b>	
Nothing found	
<b>Other Standards Bodies (ISO, ANSI, IEEE, ...)</b>	
Joint Architecture Reference Model (10 Layer)	Summary: The Joint Architecture Advisory Group (JAAG) Architecture Principles are intended to reflect an overall consensus on the guiding principles that encourage



# CGS Contingency Planning Capability



Version 1.1.1

	development of a technical architecture supporting a mutually beneficial five-eyes federation, based on a federated architectural approach.

## 10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Testing—All contingency plans need to be tested for effectiveness and security.
2. Cost of planning—Even highly unlikely contingencies need to be planned for, which can make the costs of this Capability grow.
3. Cost of contingency mechanisms—Backup systems or facilities may need to be maintained solely for contingency reasons. The costs associated with this can include power; heating, ventilation, and air conditioning (HVAC); and technology infrastructure.

## 11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Contingency Planning Capability.



# CGS Contingency Planning Capability



Version 1.1.1

- The Enterprise shall be responsible for maintaining the operations of critical systems, supporting mission-essential functions, and preventing significant loss from system or resource disruption as well as covering the technical, personnel, physical, and environmental aspects of the Enterprise in relation to information systems.
- The Enterprise shall develop contingency and continuity planning programs to meet requirements outlined in applicable standards. Enterprises shall not develop these programs independent of one another, and plans shall map to higher-level national and federal policies.
- Contributors to the contingency plan shall be knowledgeable in standards and policies, and the team shall include subject matter experts.
- Enterprises shall understand dependencies on other contingency plans and integrate their contingency and continuity planning activities in a single, efficient, and focused effort to better prepare for undesirable events.
- To develop an information system contingency plan, business and mission priorities shall be developed to define the business impact analysis to determine the system availability requirements and dependencies that are needed to make a decision regarding specific contingency solutions.
- The Enterprise shall address operations contingency planning and ensure there is a relevant contingency plan documented for every realistically foreseeable event that could affect the Enterprise.
- The information system contingency plan shall designate local and distant alternate facilities, and planning shall be done in such a way to ensure the Enterprise operates in the manner it should before, during, and after a major catastrophe.
- Information system contingency plans shall identify critical resources such as services and systems that support mission functions.
- Information system contingency plans shall map across different areas of responsibility if there are interdependencies.
- Information system contingency plans shall define what level of disruption is allowable for those resources that can withstand a disruption and within what timeframe they have to be restored. For low-critical functions, there shall be some degree of reconstitution of data.
- As a part of the contingency planning, a process shall be defined to assess incidents and decide which contingency plan shall be implemented.
- The contingency plan shall establish policy for allowable response times and policy covering mission availability fluctuations that may occur if a mission system has to be switched over to a contingency system.



# CGS Contingency Planning Capability



Version 1.1.1

- To support the restoration of disrupted services, contingency planning shall include approaches such as restoring information systems through the use of alternate equipment, potentially performing business processes through manual means, recovering information systems operations at an alternate location, and implementing appropriate contingency planning controls.
- Full-scale emergency response exercises shall be planned and conducted annually to validate that the contingency plan meets mission assurance requirements.
- Full-scale exercises shall be approved by senior management with concurrence from a mission analysis group, based on criticality and mission impact. Decision-makers shall determine, based on these factors, whether real-world testing is required.
- The contingency planning shall be continuously monitored to determine when new information system contingency planning needs arise.
- Defined contingency plans shall be reevaluated and updated annually, as necessary.
- Changes identified concerning risk analysis, mission flow, and utilization and performance management shall trigger reevaluation of contingency plans.
- The contingency planning approach shall be responsive to operational changes and tie together information such as mission criticality, resource requirements, and other information received to reassess contingency planning in a timely manner.
- Information system contingency plans shall be centrally managed.
- Contingency planning shall provide a process for distributing, and notifying interested parties of, new or updated contingency plans.
- The Enterprise shall ensure that all users receive and understand their roles and responsibilities and the purpose of the contingency plans.
- Any revisions to the contingency plan shall be communicated to relevant users through training and awareness activities.
- Information system contingency plans shall be developed in coordination with other Enterprises to maintain Enterprise interoperability and cross-Enterprise mission flow. Communication across Enterprises shall occur if there is a disruption that may affect others, to help ensure the Enterprises are prepared.