VA INFORMATION SYSTEM CONTINGENCY PLANNING

1. **REASON FOR ISSUE:** To establish operational requirements and departmental framework for the implementation of information system contingency planning, to include business impact analysis and disaster recovery planning, as required by Federal statutes (included within References) and the Department of Veterans Affairs (VA) Directive and Handbook 6500, Cybersecurity Program, dated February 24, 2021.

2. **SUMMARY OF CONTENT / MAJOR CHANGES:** This Handbook provides the procedures and operational requirements for implementing information system contingency planning in accordance with VA Directive and Handbook 6500, Cybersecurity Program, ensuring Department-wide compliance with the Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§ 3551-3554 and the security of VA information and information systems administered by or on behalf of VA. This Handbook applies to all VA organizations, their employees, and contractors working for or on behalf of VA. This Handbook includes revisions based on Federal guidance including the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems; NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations and VA Directive and Handbook 6500. These changes provide updated guidance on developing a systems-based Business Impact Analysis (BIA), an Information System Contingency Plan (ISCP), and a Disaster Recovery Plan (DRP) to meet or exceed Federal standards.

3. **RESPONSIBLE OFFICE:** Office of Information and Technology (005), Office of Information Security (005R), Information Security Risk Management (005R4).

4. **RELATED DIRECTIVE:** VA Directive 6500, VA Cybersecurity Program, dated February 24, 2021.

5. **RESCISSIONS:** VA Handbook 6500.8, Information Technology Contingency Planning, dated April 6, 2011.

CERTIFIED BY:

/s/
Nathan T. Sanfilippo
Acting Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Eddie Pool
Acting Assistant Secretary for
Information and Technology and
Chief Information Officer

DISTRIBUTION: Electronic Only

VA INFORMATION SYSTEM CONTINGENCY PLANNING

CONTENTS

PARAGRAPH **PAGE**

1. PURPOSE. 3
2. SCOPE. 3
3. ROLES AND RESPONSIBILITIES. 4
4. EXECUTIVE SUMMARY / BACKGROUND. 12
5. PROCEDURES. 15
6. REFERENCES. 19
7. APPENDIX A – Terms & Definitions 21
8. APPENDIX B – Acronyms and Abbreviation 31
9. APPENDIX C - ISCP Development Process 34

FIGURES **PAGE**

Figure 1: Impact Categories and Values 38

TABLES **PAGE**

Table 1: Business Process Descriptions (Example) 36
Table 2: Impact Categories and Values 37
Table 3: Determine MTD Gap 39
Table 4: BIA Information (Example) 40
Table 5: Resource Requirements 40
Table 6: Recovery Priorities (Example) 41

1. **PURPOSE.** The purpose of this Handbook is to describe the policy and procedures for implementing and administering the VA Office of Information and Technology (OIT) systems-based Business Impact Analysis (BIA), the Information System Contingency Plan (ISCP), and the Disaster Recovery Plan (DRP) processes. The primary objectives of this process are to:

   a. Provide a coordinated strategy to ensure information systems supporting VA critical business functions can be recovered, reported and restored following an unforeseen event or disruption.

   b. Develop an ISCP, a system-based BIA and DRPs for the assessment and recovery of an information system.

   c. Refine policies, plans and procedures to continually improve Information System (IS) contingency planning by employing an iterative program management cycle.

   d. Support the performance of VA's mission and essential functions within the National Response Framework.

   e. Establish maximum tolerable downtimes (MTDs), recovery point objectives (RPOs), recovery time objectives (RTOs), and work recovery times (WRTs) to ensure VA IS services and assets supporting VA essential business functions can be recovered and restored following a disruption.

2. **SCOPE**.

   a. VA Handbook 6500.8 satisfies the Federal and statutorily requirements of:

      (1) Federal Information Security Modernization Act (FISMA);

      (2) U.S. Code (U.S.C.) Title 38, Veterans' Benefits Act, Subchapter III – Information Security; and

      (3) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Contingency Planning Guide for Federal Information Systems.

   b. VA Handbook 6500.8 addresses the procedural elements of OIT ISCP activities and provides prescriptive guidance for all VA information technology (IT) that receive, process, store, display, or transmit VA information. These technologies are broadly grouped as VA Information Systems, Platform IT, cyber physical systems, IT services, and IT products. This includes IT supporting research, development, test and evaluation, IT operated by a contractor or other entity on behalf of VA, and electronic health records. This also includes Managed Services that are required to have an ATO under VA Directive 6500 and that follow the contract security process initiated by VA Handbook 6500.6. Contingency Planning for Medical Devices, as defined by VA Directive 6550, will be addressed through established procedures.

c. Nothing in this handbook alters or supersedes the existing authorities and policies of VA and other Federal laws and regulations.

3. **ROLES AND RESPONSIBILITIES**. This Handbook defines roles and responsibilities, as it relates to IS contingency planning, to boost operational efficiency and optimize redundancies.

a. **VA Assistant Secretary for Information and Technology (AS IT) / VA Chief Information Officer (CIO)** shall oversee the implementation of this Handbook as a supplement to VA Handbook 6500, and shall:

(1) Direct and oversee the IS contingency planning and test training, exercise and activation of Continuity of Operations (COOP) of VA IT;

(2) Distribute standards and sharing requirements; and

(3) Act as the approval authority for OIT for all ISCPs.

b. **Deputy Assistant Secretary for the Office of Information Security (DAS OIS) / VA Chief Information Security Officer (CISO)** shall:

(1) Advise and assist the VA AS IT/VA CIO on matters related to information security, including IS and business continuity planning;

(2) Develop and maintain information security policies, procedures, and control techniques to address system security planning as described in VA Directive 6500;

(3) Manage the identification, implementation, and assessment of common security controls; and

(4) Ensure training of personnel with significant Business Impact Analysis (BIA), ISCP, or DRP responsibilities.

c. **VA Office of Human Resources and Administration / Operations, Security and Preparedness (HRA/OSP) Office of Emergency Management and Resilience (OEMR)** shall:

(1) Develop and maintain the VA Master Continuity Plan;

(2) Develop, coordinate, and implement policy and programs to ensure the VA has an integrated Comprehensive Emergency Management Program;

(3) Provide required biannual reviews and identification of VA’s Primary Mission Essential Functions (PMEFs) and Mission Essential Functions (MEFs) for use in established Business Process Analysis (BPA) and BIA validation processes. This is done in accordance with Presidential Policy

Directive 40 (PPD-40), National Continuity Policy and relevant Federal Continuity Directives (FCDs);

(4) Operate the Integrated Operations Center (IOC), to include recording and monitoring Federal Emergency Management Agency (FEMA) Mission Assignment (MA) requests for additional disaster response resources. MAs are task orders issued by FEMA to other Federal agencies that allow for additional resources to be committed in response to a disaster;

(5) Provide and manage continuity communication capabilities and equipment when needed; and

(6) Coordinate activities to prepare VA senior leaders and staff for Eagle Horizon exercises.

d. **VA Information Security Risk Management (ISRM)** shall:

(1) Develop, update, maintain, and provide oversight to VA information system level Contingency Planning (CP) procedures and standard templates for systems-based BIAs, ISCPs, and DRPs;

(2) Develop, update, and maintain guidance on VA CP requirements based on information system type. Guidance, including standard operating procedures and manuals, will be posted on the VA Knowledge Service, will contain expectations for key stakeholders in the CP process, and will provide requirements for types of information systems;

(3) Conduct final review of information system level ISCPs and associated documents;

(4) Develop and maintain a process for ensuring all ISCPs and associated documents, are reviewed, approved, and uploaded into the VA Governance, Risk and Compliance (GRC) tool;

(5) Facilitate the creation of a process and developing guidance and procedures to define IS support and alignment to VA MEFs and PMEF;

(6) Develop, update, and maintain guidance on how to determine the MTD, RPO, RTO, and WRT for an IS based upon business requirements and the criticality of the system;

(7) Identify, organize, review, and update VA CP controls, including preventative controls, in the VA GRC tool and the VA Knowledge Service Security Controls Explorer as new directives and agency strategies are published;

(8) Develop, update, and maintain guidance and oversight for testing, training, exercise and evaluation (TTE&E) of information system level Contingency Plans and related CP documents; and

(9) Coordinate with system stakeholders to ensure that each IS is properly tested in accordance with their Federal Information Processing Standards (FIPS) 199 security categorization and approved ISCP.

e. **VA OIT Enterprise Command Center (ECC)** shall:

(1) Monitor systems for potential or actual system disruptions and outages; and

(2) Provide early notification to stakeholders, when possible, for action.

f. **VA OIT Enterprise Command Operations (ECO)** shall:

(1) Conduct trend analysis and higher-level review of overall RTO information of an IS, upon request; and

(2) Provide executive leadership during large scale outages where ISCP and DRPs are used.

g. **VA OIT Office of Emergency Management (OEM)** shall:

(1) Provide testing support as available to ISOs for systems with medium or high availability (HA) ratings with the requirement to functionally test their ISCPs and DRPs annually; and

(2) Provide emergency communications, when required, during an incident. These communications may include cellular routers, satellite phones, and Very Small Aperture Terminals (VSATs).

h. **VA OIT Major Incident Management (MIM)** shall:

(1) Own and maintain the incident escalation process that is used during disruptive events;

(2) Provide stakeholders within the ISCP Point of Contact (POC) list with guidance on the incident escalation process; and

(3) Assist ISCP Coordinators during disruptive events by capturing incident data as it relates to system recovery metrics.

i. **VA OIT IT Program Integration Continuity and Mission Assurance (ITPI CMA)** shall:

(1) Execute the direction of OIT's CIO, for COOP, in accordance with presidential policy, Federal executive branch interagency directives and applicable VA directives;

(2) Develop and maintain the OIT senior executive COOP plans, policies, procedures, TTE&E activities, and OIT's alternate operating location(s); and

(3) Implement the VA's mission resiliency strategy across the department; accountable and responsible for the execution of the OIT employee accountability process prior to, during, and after an emergency event on behalf of the CIO.

j. **VA Enterprise Network (VAEN)** shall coordinate with and supporting VA Area Managers to ensure the VA area infrastructure is brought back online in the event of a disaster that requires the activation of the DRP.

k. **VA Infrastructure Operations (IO)** shall, in coordination with VA data centers and VA Enterprise Cloud (VAEC) Cloud Infrastructure, ensure the supporting infrastructure and data backups are brought back online in the event of a disaster that requires the activation of the DRP.

l. **Information System Owners (ISO)** shall:

(1) Designate an individual to fulfill the role of ISCP Coordinator for each IS. The ISO will be the ISCP Coordinator if they do not designate a different individual. The Information System Security Officer (ISSO) will not be selected as the ISCP Coordinator.

(2) Identify subject matter experts (SMEs) for the ISCP POC list and ensuring that the POC list is updated. An individual may be required to fulfill multiple roles on the ISCP POC list.

(3) Ensure the systems-based BIA is conducted and approved by helping to identify and prioritize IS components critical to supporting the organization's mission/business essential functions;

(4) Validate MTD, RPO, RTO, and WRT information for existing ISs under their purview based upon business requirements and the criticality of the system;

(5) Ensure results from the systems-based BIA are appropriately incorporated into the analysis and strategy development efforts for the IS's ISCP, COOP plans, BCP, and DRP;

(6) Execute the CP process in accordance with the CP controls and other security controls which are further described in Step 3 of the ISCP development process;

(7) Coordinate with the ISCP Coordinator and DRP Director to develop a DRP and ensure its effective implementation;

(8) Ensure ISCPs are coordinated with the hosting facility and other continuity-related plans such as the COOP plans, BCP, and OEP;

(9) Integrate CP into applicable steps of the System Development Life Cycle (SDLC) and the process for obtaining Authorization to Operate (ATO);

(10) Review and approving completed and updated systems-based BIAs, ISCPs, and DRPs;

(11) Ensure completed and updated systems-based BIAs, ISCPs, and DRPs are uploaded into the VA GRC tool;

(12) Activate the ISCP in the event of a known or suspected outage;

(13) Notify ISCP Coordinator and other appropriate members of the ISCP POC list required to respond to a given incident as required by the circumstances of the incident;

(14) Draft and release notifications upon the determination of an outage, upon the return to normal operations, and when recovery efforts are complete;

(15) Ensure the TTE&E process is completed as described in Section 5.f, ISCP Development Process Step 6: Ensure ISCP TTE&E;

(16) Develop a test plan designed to examine the ISCP against explicit test objectives and success criteria based on VA policy;

(17) Coordinate with the ISCP Coordinator on the type of CP test or exercise to be conducted at least once annually to validate ISCP effectiveness;

(18) Secure budget and resource allocations necessary for conducting simulated or functional CP tests and exercises, as well as capacity planning where necessary; and

(19) Complete, in coordination with the ISCP Coordinator, After-Action Reports (AARs) after the CP test or exercise is performed, updating the ISCP and the CP controls where gaps are identified, and ensuring the CP deliverables are certified and uploaded into the VA GRC tool.

m. **The Business Owner, also referred to as the Mission Owner in VA Directive 6500** shall:

(1) Support the ISCP Coordinator in the development of the systems-based BIA;

(2) Provide input to the development ISCP including in the creation of contingency strategies; and

(3) Participate in the testing of ISCP.

n. **Information System Security Officer (ISSO)** shall:

(1) Conduct initial review of the systems-based BIAs and ISCPs of each IS under their purview at least annually;

(2) Participate in the completion of the systems-based BIA, ISCP, and DRP for each IS under their purview;

(3) Ensure CP training is performed at least annually to prepare the system's CP stakeholders to respond promptly to future events;

(4) Participate in the testing of the ISCP and DRP for each IS under their purview;

(5) Support the ISO in maintaining documentation of the CP TTE&E activities, dates, locations, and personnel for audit trail purposes and future reference; and

(6) Oversee the day-to-day continuity program, representing ISs at interagency forums and working groups, as appropriate, and ensuring continuity personnel are properly trained and facilities properly equipped to execute ISCPs with little or no notice.

o. **Information System Security Manager (ISSM)** shall:

(1) Assist the ISO, ISSO, ISCP Coordinator and DRP Director with the creation of systems-based BIAs, ISCPs, and DRPs;

(2) Report the systems-based BIA, ISCP, and DRP posture of ISs to the AO and other organizational officials on an ongoing basis, as documented in the VA Knowledge Service Security Controls Explorer, in accordance with VA Risk Management Framework (RMF) strategy;

(3) Coordinate with organizational managers to ensure a coherent, coordinated and holistic approach to the ISCP across the operational units;

(4) Ensure that cybersecurity inspections, tests and reviews, including those for CP TTE&E, are coordinated for the network environment in accordance with the timeframe documented in the VA Knowledge Service Security Controls Explorer;

(5) Ensure that security improvement actions, including those identified during ISCP TTE&E activities, are documented evaluated, validated, and

implemented as required in accordance with the timeframe documented in the VA Knowledge Service Controls Explorer;

(6) Interpret patterns of noncompliance with systems-based BIA, ISCP, and DRP policy to determine their impact on levels of risk and/or overall effectiveness of the enterprise's system-based BIA, ISCP and DRP program; and

(7) Ensure systems-based BIA, ISCP, and DRP activities are incorporated into the security assessment and authorization process.

p. **Information System Contingency Plan (ISCP) Coordinator** shall:

(1) Designate an ISCP Coordinator (alternate) to act on behalf of the ISCP Coordinator if the ISCP Coordinator is unavailable;

(2) Conduct the systems-based BIA for each IS using the template found on the VA Knowledge Service and discussed in Section 5.b, ISCP development process Step 2: Conduct the BIA;

(3) Manage the development and execution of the ISCP for each IS to which they have been appointed;

(4) Review each systems-based BIA and ISCP annually, updating as necessary and ensuring that information in each document is current and meets system and policy requirements;

(5) Review system recovery measures and technologies to meet the recovery priorities;

(6) Ensure, as part of the ISCP development, that the IS's security, management, operational and technical controls are equivalent with a prospective alternate processing or storage sites;

(7) Ensure that the ISCP strategy chosen can be implemented effectively with available personnel and financial resources;

(8) Designate appropriate POCs from the ISCP POC list to implement the CP strategy;

(9) Implement the steps of the ISCP in the event of an outage.

(10) Coordinate with the ISO and DRP Director to develop a DRP and ensure its effective implementation;

(11) Inform, upon receiving outage information from ECC or other stakeholders including external entities such as a cloud service provider and in

coordination with the Outage and Damage Assessment Lead, the ISO when activation criteria have been met;

(12) Support the ISO in developing a test plan designed to examine the ISCP against explicit test objectives and success criteria based on VA policy;

(13) Coordinate with the ISO on the type of CP test or exercise to be conducted at least once annually to validate ISCP effectiveness;

(14) Complete, in accordance with the timeframes defined in the VA Knowledge Service Security Controls Explorer and in coordination with the ISO, AARs after the CP test or exercise is performed;

(15) Update the ISCP, DRP, and the CP controls based on gaps identified in the CP testing in accordance with the timeframes defined in the VA Knowledge Service Security Controls Explorer;

(16) Document after every IS outage all actions related to the outage including all actions taken during the activation and notification phase, the recovery phase and the reconstitution phase, the AAR including lessons learned and all notifications. Documentation should be done in accordance with the timeframes defined in the VA Knowledge Service Security Controls Explorer;

(17) Coordinate with CMA ITPI and Business Owners to identify essential mission, service and business functions;

(18) Coordinate with ISSOs to ensure that impacts caused by changes within the organization will be reflected in the ISCP; and

(19) Evaluate supporting information to ensure that the information is current and meets system requirements. This information includes, but is not limited to, alternate processing site contracts, alternate storage site contracts, software licenses, Service -Level Agreements (SLAs), Memoranda of Understanding (MOUs), hardware/software requirements, Interconnection Security Agreements (ISAs), security requirements, recovery strategies, contingency policies, training and awareness materials, testing scope and other plans such as COOP plans and BCPs.

q. **Information System Contingency Plan Coordinator (Alternate)** shall:

(1) Act as the ISCP Coordinator when the ISCP Coordinator is unavailable; and

(2) Perform the responsibilities of the ISCP Coordinator.

r. **Disaster Recovery Plan (DRP) Director**. The DRP Director shall:

(1) Develop, execute, maintain, activate and deactivate the system-level DRPs;

(2) Determine if alternate manual or secondary processing should be initiated as a temporary method of maintaining business operations; and

(3) Designate a DRP Director (alternate) to act as the DRP Director if the DRP Director is unavailable.

s. **Disaster Recovery Plan (DRP) Director (Alternate)** shall:

(1) Act as the DRP Director when the DRP Director is unavailable; and

(2) Perform the responsibilities of the DRP Director.

4. **EXECUTIVE SUMMARY / BACKGROUND.** VA Handbook 6500.8 establishes the ISCP and defines the plan objectives to guide responsible parties through the ISCP development process. This includes designing a contingency planning program and evaluating the organization's needs against contingency strategy options based on a system's RMF impact levels.

a. **ISCP Development Process** comprises a coordinated recovery strategy after a disruption and is conducted in accordance with the seven-step ISCP process outlined in NIST SP 800-34, Revision 1, Chapter 3, Page 13, Contingency Planning Guide for Federal Information Systems.

(1) Refer to NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, Figure 3-1: Contingency Planning Process for an illustration of the Contingency Planning (CP) Process.

(2) The CP process begins during the Initiation phase of the Software Development Life Cycle (SDLC) and is integrated throughout the SDLC. Refer to VA Handbook 6500.5, Incorporating Security and Privacy into the System Development Life Cycle and NIST SP 800-34 Appendix F, Contingency Planning and the SDLC, for more detailed information on the SDLC. Once the ISCP is developed, it must be reviewed and updated on an annual basis or when any major changes to the system are made. Major changes are any modifications to the system that requires a new ATO.

b. **ISCP Requirements** is in accordance with FISMA, NIST SP 800-34, NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-84, Guide to TTE&E programs for IT Plans and Capabilities. These requirements fulfill the following CP controls:

(1) Developing, documenting, and disseminating a CP policy providing the authority and guidance necessary to develop an effective ISCP, including the requirement to complete a systems-based BIA;

(2) Developing, documenting, and disseminating CP procedures, including the development of a systems-based BIA, to facilitate the implementation of the CP policy and associated controls;

(3) Defining the TTE&E procedures, documenting and reviewing the TTE&E results and initiating corrective actions, if needed;

(4) Ensuring IS-level CP training is provided to improve system stakeholders and organization-wide preparedness for ISCP activation. This should include a TTE&E plan to validate recovery capabilities and identify planning and execution gaps.

(5) Ensuring establishment of an alternate capability for VA ISs;

(6) Establishing alternate telecommunication services, including necessary agreements to permit the resumption of defined IS operations for essential missions and business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites;

(7) Ensuring the establishment of an alternate storage site for all VA ISs, including necessary agreements to permit the storage and retrieval of IS backup information and ensuring that the alternate storage site provides information security safeguards equivalent to those of the primary site;

(8) Ensuring backups are conducted for both user-level and system-level information in accordance with the IS and IS documentation, consistent with RTO, RPO, MTD, and WRT;

(9) Ensuring that all VA ISs have readily available ISCPs with thorough contingency strategies and resource capabilities necessary to support quick and effective system recovery within the RPO.

c. **RMF** emphasizes risk management by promoting the development of security and privacy capabilities into ISs throughout the SDLC as described in NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Chapter 1.1 and 2.2.

d. **Phases of Contingency Response** consists of three primary phases (activation / notification phase, recovery phase and reconstitution phase) that must be addressed in the ISCP as defined in NIST SP 800-34 Revision 1, Chapter 4.

e. **ISCP Background Information:** An ISCP establishes procedures for the assessment and recovery of an IS following a system disruption or outage. It provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures and testing procedures for a system. Before reviewing the

ISCP development process one should be familiar with the key information that is encompassed in the ISCP structure and format. This section will provide guidance on the information and details that are part of an ISCP. Additional guidance can be found in the ISCP template hosted on the VA Knowledge Service website.

(1) **ISCP Goals and objectives** should begin by outlining the IS's contingency objectives and establishing the responsibilities for their specific contingency planning tasks. These goals and objectives should be aligned with higher level VA and VA OIT objectives and essential functions, along with the relevant policies listed in References.

(2) **ISCP Authority / Approval:** Each ISCP must outline and clearly identify under whose authority and approval the ISCP and subsequent contingency planning actions and associated documentation is established to certify the ISCP:

(a) is complete and provides an accurate representation of the IS, including its hardware, software, and telecommunications components;

(b) identifies the criticality of the IS as it relates to the mission of the organization and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality;

(c) will remain in accordance with Federal regulations and guidance listed in references to include VA Handbook 6500.8 guidance; and

(d) will be tested and reported annually.

(3) **ISCP System Information:** The ISCP should include general description of the IS addressed by the plan to include, but not limited to:

(a) IS name;

(b) operating environment;

(c) physical location;

(d) general location of users;

(e) partnerships with external organizations/systems;

(f) information regarding any other technical considerations that are important for recovery purposes, such as backup procedures; and

(g) a diagram of the architecture, including inputs, outputs, telecommunications connections, and security devices (e.g., firewalls, internal and external connections).

(h) Note: The content for the system description can be found in the VA's GRC tool. Refer to the GRC tool process documentation.

(4) **Identifiers:** Each ISCP must identify critical information that aligns with the system identifiers in the VA GRC tool and includes:

(a) the IS name;

(b) the IS abbreviation; and

(c) the unique identifier (e.g., GRC tool ID or FedRAMP application number if applicable).

(5) **Authorization Boundaries** include all IS components, including hardware, firmware and software. All ISs must have their authorization boundary clearly identified. This includes system types that belong to each specific boundary before plans are created. All ISs with an overall defined FIPS 199 security impact categorization must have corresponding ISCPs. The authorization boundary should include identification of supporting applications that the IS is reliant upon. Guidance on authorization boundaries can be found on the VA Knowledge Service.

(6) **Points of Contact:** Each ISCP should have clearly defined POCs identified. This includes all personnel that will be notified and activated in the event of a service disruption. The POC list as an appendix to the ISCP should be reviewed and updated according to federal guidance to ensure all personnel can be reached during an activation.

f. **Coordination of Department-wide policies and programs:** The ISCP fits into a much broader security and emergency management effort that includes organizational and business processes continuity of operations program, disaster recovery planning and incident management. The ISCP shall be written in coordination with plans associated with each target system as part of a Department-wide resilience strategy, as defined in NIST SP 800-34 Revision 1, Chapter 3.

5. **PROCEDURES**. ISCP Development Process.

a. **Step 1 - IS Contingency Planning Policy**: The first step of the ISCP development process is to develop the policy that is the basis for all IS contingency planning efforts. It is the responsibility of VA OIT to draft, review, and maintain IS contingency planning policy and guidance. This Handbook, in addition to other regulations, shall be reviewed and confirmed annually to ensure it is aligned with policies in Section 6. In addition to this Handbook, contingency

planners should review the requirements and guidance listed in the VA Knowledge Service website such as CP requirements based on information system type.

b. **Step 2 - Conduct the BIA:**

(1) The systems-based BIA is used to characterize the impacts and consequences of a disruption to the system components, supported mission/business processes, and interdependencies. The systems-based BIA is used as the foundation to determine IS contingency planning requirements and priorities. Results from the systems-based BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's COOP plan, BCPs, and DRP.

(2) The systems-based BIA should be performed during the initiation phase of the SDLC. As the system design evolves and components change, the systems-based BIA may need to be conducted again during the development/acquisition phase of the SDLC. Additionally, once the system reaches the maintenance phase, the systems-based BIA should be reviewed and verified annually to ensure the specifics of the systems-based BIA have not changed. See Appendix C for additional details about process-based BIA vs. systems-based BIA.

c. **Step 3 - Identify Security Controls and Preventive Measures:** Identify, assess and establish security controls and preventive measures to minimize the impact of disruptions on the IS. The System Security Plan (SSP) is where the implementation of the security controls is documented. The SSP also includes a description of the system's functionality and physical environment as well as identified findings for any vulnerabilities. The SSP serves as a companion to the ISCP. Changes that are made to the SSP, including major changes in the system's security posture or changes to the system environment, will require a review and updates to the ISCP.

d. **Step 4 - Create Contingency Strategies** to mitigate and address the impacts from a disruption to an IS. This includes establishing backups and recovery procedures to minimize the downtime of a system. Recommended standards for backups, recovery and reconstitution planning in the ISCP can be found in Appendix C.

e. **Step 5 - Develop ISCP and DRP:** Once the IS contingency planning policy has been developed, the systems-based BIA has been completed and ISCP controls have been identified, an ISCP and DRP, if applicable, will be developed for each IS, including minor applications. An ISCP and DRP:

(1) must be completed for all ISs within an authorization boundary. These ISs must complete an ISCP, DRP, and all associated plans, including systems-based BIAs;

(2) must be developed by the ISCP Coordinator and DRP Director using the ISCP and DRP templates and guidance, including standard operating procedures and manuals, as found on the VA Knowledge Service;

(3) must be uploaded into the VA GRC tool by the ISO or generated/inputted in the VA GRC tool using the ISCP automated template; and

(4) must be reviewed and approved on an annual basis by the ISO.

f. **Step 6 – Ensure the ISCP TTE&E Program** is maintained, improved upon, documented, and defined at least annually in accordance with VA Directive 0324, *TTE&E Program*, NIST SP 800-34 Rev. 1 Chapter 3.5, and NIST SP 800-84.

(1) Exercise Planning. Annual ISCP testing and exercising is required for all systems to determine the plan's effectiveness and VA's readiness to execute the plan. All tests and exercises should include a determination of the effects on VA's operations and provide for a mechanism to improve the plan as a result. The type of test or exercise required is based on the information system's FIPS 199 impact level.

(a) Low-impact systems require an annual tabletop exercise.

(b) Moderate-impact systems must conduct a functional exercise to satisfy the first contingency plan testing requirement. A tabletop exercise is acceptable in the following two years. This contingency plan testing cycle repeats every three years. Any IS that has significant changes or edits to their ISCP must restart the cycle and conduct a functional exercise before any tabletop exercises.

(c) High-impact systems require a functional exercise to be conducted annually.

g. **Step 7 – Plan Maintenance:** Once the ISCP has been developed, implementation and continuous monitoring must begin. Certain aspects can be modified according to the needs and requirements of the organization, so the ISCP must be reviewed and updated annually.

(1) **Reviews and Updates**: The ISCP will require updates and reviews performed relative to the different segments:

(a) the operational requirements for the plan;

(b) security needs;

(c) the technical processes;

(d) the amount, specification, and types of the hardware equipment, software entities, Hardware Bill of Materials (HBOM), Software Bill of Materials (SBOM), and other equipment relevant for the plan;

(e) the names and contact details for the personnel and teams;

(f) the names and contact information for all the vendors, with inclusion of both the alternate data storage facility and alternate COOP plan/DRP site; and

(g) essential records, both electronic and hard copy.

(2) **Disclosure and Authorization:** The organization should ensure that the disclosure and authorization forms and specifications are updated and reviewed regarding the existing industry standards and requirements.

(3) **Coordination within Internal and External Organizations**: Any changes or updates to the ISCP need to be coordinated with internal and external organizations. The ISCP Coordinator will be tasked with conducting coordination for the following information with applicable internal and external organizations as identified in the ISCP:

(a) alternate processing site;

(b) alternate storage site;

(c) software licenses;

(d) MOU's, SLAs, and any other agreements made by the organization;

(e) hardware and software system requirements;

(f) security needs and adherences;

(g) recovery plan and strategy;

(h) contingency policies;

(i) training operations and availability of awareness materials;

(j) testing procedures; and

(k) any other plans that the organization has (e.g., COOP plan or BCP).

(4) Distribution and Changes

(a) Copies of the fully typed ISCP will be stored:

i by the recovery team;

ii at the alternate storage and processing sites; and

iii on backup systems.

(b) The completed ISCP contains controlled unclassified information and must be version controlled. Distribution must be controlled to prevent unauthorized disclosure and modification given the sensitive information about the organization and the recovery personnel.

(c) The systems-based BIA must be updated with any new information, details, and requirements.

(d) The ISCP will be updated to include new technologies and when outdated hardware/software is disposed of.

6. **REFERENCES.**

a. **Statutes and Regulations.**

(1) Presidential Policy Directive – 40, National Continuity Policy, July 15, 2016.

(2) National Response Framework, October 28, 2019.

(3) Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017.

(4) Federal Information Security Modernization Act of 2014, 44 United States Code (U.S.C.) § § 3541-3549 and 3554.

(5) Administrative Safeguards of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, 45 Code of Federal Regulations (C.F.R.) §164.308.

(6) The Privacy Act of 1974, 5 USC §552a.

b. **Federal Information Processing Standards (FIPS) Publications.**

(1) FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems.

(2) FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

c. **National Institute of Standards and Technology (NIST) Special Publications (SP).**

(1) NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems.

(2) NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments.

(3) NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.

(4) NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations.

(5) NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations.

(6) NIST SP 800-84, Guide to Test, Training and Exercise Programs for IT Plans and Capabilities.

d. **Office of Management and Budget (OMB) Publications.**

(1) OMB Circular A-130, Appendix III, Management of Federal Information Resources, November 2000.

e. **VA Directives and Handbooks.**

(1) VA Directive 0320, VA Comprehensive Emergency Management Program.

(2) VA Handbook 0324, Test, Training, Exercise and Evaluation Program.

(3) VA Directive 6500, VA Cybersecurity Program.

(4) VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program.

f. **Other References.**

(1) VA Information Security Knowledge Service Portal.

(2) Federal Emergency Management Agency (FEMA) Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements.

(3) FEMA Federal Continuity Directive 2 – Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process.

(4) FEMA Guide to Continuity Program Management.

APPENDIX A – Terms & Definitions.

1. **After-Action Report (AAR):** A document containing findings and recommendations from an exercise or a test. SOURCE: NIST SP 800-84.

2. **Alternate Sites:** Storage or processing sites that are geographically distinct from the primary storage or processing sites where leadership and continuity personnel relocate to perform essential functions following activation of the continuity plan. SOURCE: NIST SP 800-53.

3. **Authorization Boundary:** All components of an IS to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the IS is connected. SOURCE: NIST SP 800-53.

4. **Authorization to Operate (ATO):** The official management decision given by a senior Federal official or officials to authorize operation of an IS and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency ISs. SOURCE: NIST SP 800-53.

5. **Authorizing Official (AO):** A senior Federal official or executive with the authority to authorize the operation of an IS or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image or reputation), agency assets, individuals, other organizations and the Nation. SOURCE: NIST SP 800-53.

6. **Availability:** Ensuring timely and reliable access to and use of information. SOURCE: FIPS 199.

7. **Backup:** A copy of files and programs made to facilitate recovery if necessary. SOURCE: NIST SP 800-34.

8. **(Control) Baseline:** The set of controls that are applicable to information or an IS to meet legal, regulatory or policy requirements, as well as address protection needs for the purpose of managing risk. SOURCE: NIST SP 800-37.

9. **Business Continuity Plan (BCP):** The documentation of a predetermined set of instructions or procedures that describe how an organization’s mission/business processes will be sustained during and after a significant disruption. SOURCE: NIST SP 800-34.

10. **Business Impact Analysis (BIA):** An analysis of an IS’s requirements, functions and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. SOURCE: NIST SP 800-34.

11. **Business Process Analysis (BPA):** A method of examining, identifying and mapping the functional processes, workflows, activities, personnel expertise, systems, data, interdependencies and alternate locations inherent in the execution of a function or requirement. SOURCE: FCD 1.

12. **Capability:** A combination of mutually reinforcing controls implemented by technical means, physical means and procedural means. Such controls are typically selected to achieve a common information security or privacy purpose. SOURCE: NIST SP 800-37.

13. **Common Control Provider:** An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., controls inheritable by organizational systems). SOURCE: NIST SP 800-37.

14. **Common Control:** A security or privacy control that is inherited by multiple ISs or programs. SOURCE: NIST SP 800-37.

15. **Common Security Control:** Security control that can be applied to one or more agency ISs and has the following properties:

    a. the development, implementation and assessment of the control can be assigned to a responsible official or organizational element (other than the ISO); and

    b. the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency IS where that control has been applied. SOURCE: NIST SP 800-18.

16. **Component (Organization):** A sub-organization or directorate that supports HQ leadership in the performance of PMEFs and/or MEFs, by performing those MEFs and/or ESAs required to complete a PMEF or National Essential Function (NEF). Examples of a component could be an agency, bureau, regional office, district office and/or a local office. SOURCE: FCD 1.

17. **Contingency Planning (CP):** The process of developing an overall program for achieving continuity of operations for organizational mission and business functions. CP addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. CP is considered throughout the system development life cycle and is a fundamental part of the system design. SOURCE: NIST SP 800-53.

18. **Continuity:** The ability to provide uninterrupted services and support, while maintaining organizational viability, before, during and after an event that disrupts normal operations. SOURCE: FCD 1.

19. **Continuity of Operations (COOP) Plan:** A predetermined set of instructions or procedures that describe how an organization’s mission essential functions will be

sustained within 12 hours and for up to 30 days because of a disaster event before returning to normal operations. SOURCE: NIST SP 800-34.

20. **Continuity Plan**: A documented plan that details how an individual organization will ensure it can continue to perform its essential functions during a wide range of events that impact normal operations. SOURCE: FCD 1.

21. **Continuous Monitoring:** Maintaining ongoing awareness to support organizational risk decisions. SOURCE: NIST SP 800-37.

22. **Disaster Recovery Plan (DRP):** A written plan for recovering one or more ISs at an alternate facility in response to a major hardware or software failure or destruction of facilities. SOURCE: NIST SP 800-34.

23. **Disruption:** An unplanned event that causes an IS to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network or equipment or facility damage or destruction). SOURCE: NIST SP 800-34.

24. **Enterprise:** An organization with a defined mission/goal and a defined boundary, using systems to execute that mission and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, human resources, financial management, security and systems, or information and mission management. See organization. SOURCE: NIST SP 800-37.

25. **Essential Functions**: A subset of government functions that are determined to be critical activities. These essential functions are then used to identify supporting tasks and resources that must be included in the organization's continuity planning process. In this document, the term "essential functions" refers to those functions an organization must continue in a continuity situation, whether the functions are mission essential functions, primary mission essential functions or essential supporting activities. SOURCE: FCD 1.

26. **Essential Records:** ISs and applications, electronic and hard copy documents, references and records needed to support essential functions during a continuity event. The two basic categories of essential records are emergency operating records and rights and interest records. Emergency operating records are essential to the continued functioning or reconstitution of an organization. Rights and interest records are critical to carrying out an organization's essential legal and financial functions and vital to the protection of the legal and financial rights of individuals who are directly affected by that organization's activities. The term "vital records" refers to a specific subset of essential records relating to birth, death and marriage documents. SOURCE: FCD 1.

27. **Essential Supporting Activities (ESAs):** Functions that support performance of MEFs but do not reach the threshold of MEFs or PMEFs. ESAs are important facilitating activities performed by most organizations (e.g., providing a secure workplace, ensuring computer systems are operating); however, the sole

performance of ESAs does not directly accomplish an organization's mission. SOURCE: FCD 1 and 2.

28. **Event:** Any observable occurrence in a network or IS. SOURCE: NIST SP 800-37.

29. **Exercise:** A simulation of an emergency designed to validate the viability of one or more aspects of an ISCP. SOURCE: NIST SP 800-84.

30. **Federal Continuity Directive (FCD):** A document developed and promulgated by DHS/FEMA, in coordination with the Continuity Advisory Group and in consultation with the Continuity Policy Coordination Committee, which directs executive branch organizations to carry out identified continuity planning requirements and assessment criteria. SOURCE: FCD 1.

31. **Firmware:** Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. See hardware and software. SOURCE: NIST SP 800-37.

32. **High Availability:** A failover feature to ensure availability during device or component interruptions. SOURCE: NIST SP 800-113.

33. **Hybrid Control:** A security or privacy control that is implemented for an IS in part as a common control and in part as a system-specific control. See common control and system-specific control. SOURCE: NIST SP 800-37.

34. **Impact Level:** High, Moderate, or Low security categories of an IS established in FIPS 199 which classify the intensity of a potential impact that may occur if the IS is jeopardized. Also referred to as Impact Value. SOURCE: NIST SP 800-34.

35. **Improvement Plan:** The part of the AAR that identifies specific corrective actions, assigns them to responsible parties and establishes targets for their completion.

36. **Incident:** An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an IS; or constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use policies. SOURCE: NIST SP 800-37.

37. **Information Resources:** Information and related resources, such as personnel, equipment, funds and information technology. SOURCE: NIST SP 800-18.

38. **Information Security Policy:** Aggregate of directives, regulations, rules and practices that prescribes how an organization manages, protects and distributes information. SOURCE: NIST SP 800-18.

39. **Information System Contingency Plan (ISCP):** Management policy and procedures designed to maintain or restore business operations, including computer

operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. SOURCE: NIST SP 800-34.

40. **ISCP Coordinator:** Individual who develops the CP strategy for an IS in cooperation with the ISO, ISSO, and other individuals associated with the IS. ISCP Coordinator also manages development and execution of the ISCP. SOURCE: NIST SP 800-34.

41. **Information System Owner (ISO):** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an IS. SOURCE: NIST SP 800-18.

42. **Information System Security Officer (ISSO):** Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or ISO for ensuring that the appropriate operational security posture is maintained for an IS or program. SOURCE: NIST SP 800-18.

43. **Integrity:** Guarding against improper information modification or destruction. Includes ensuring information non-repudiation and authenticity. SOURCE: FIPS 199.

44. **Knowledge Service (KS):** The Knowledge Service is a dynamic online knowledge base, supports RMF implementation, planning, and execution by functioning as the authoritative source for VA security control baselines, security control descriptions, security control overlays, and implementation guidance and assessment procedures. SOURCE: VA Handbook 6500.

45. **Maximum Tolerable Downtime (MTD):** The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission. SOURCE: NIST SP 800-34.

46. **Medical Device/System:** A non-IT device or system that meets one or more of the following requirements: (1) Is used in patient healthcare for diagnosis, treatment (therapeutic), or physiological monitoring of patients. This includes server-based medical equipment and clinical systems. Examples of medical devices/systems include, but are not limited to, physiological monitoring systems, ventilators, infusion pumps, Computed Tomography (CT) scanners, MUSE™ cardiology information systems, Picture Archiving and Communication Systems (PACS), Clinical Information Systems (CIS), and laboratory analyzers. This includes medical devices/systems that directly connect to a patient, process human and other biologic specimens, create medical images, display electrophysiological waveforms, obtain physiologic measurements, and/or directly perform therapeutic-support to the patient. (2) Has gone through the Food and Drug Administration's (FDA) Premarket Review or 510(k) Process. (3) Is incorporated as part of a medical device system in such a fashion that, if modified, the device or system component could have a negative impact on the functionality or safety of the main medical device/system. SOURCE: VA Directive 6550.

47. **Memorandum of Understanding (MOU):** Written agreements between organizations that require specific goods or services to be furnished or tasks to be accomplished by one organization in support of the other. SOURCE: FCD 1.

48. **Mission Essential Functions (MEFs):** The essential functions directly related to accomplishing an organization's mission as set forth in statutory or executive charter. Generally, MEFs are unique to each organization. SOURCE: FCD 2.

49. **National Continuity Policy:** It is the policy of the United States to maintain a comprehensive and effective continuity capability, composed of COOP and Continuity of Government (COG) programs, to ensure the preservation of our form of government under the Constitution and the continuing performance of NEFs under all conditions (PPD-40, National Continuity Policy). SOURCE: FCD 1.

50. **National Essential Functions (NEFs):** Select functions necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and COG capabilities. SOURCE: FCD 1 and 2.

51. **Non-repudiation:** Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. SOURCE: NIST SP 800-18.

52. **Normal Operations:** Refers to the broad functions undertaken by an organization; these functions include day-to-day tasks, planning and execution of tasks. May also be referred to as steady-state operations. SOURCE: FCD 1.

53. **Occupant Emergency Plan (OEP):** A short-term emergency response plan which establishes procedures for evacuating buildings or sheltering-in-place to safeguard lives and property. Organizations may refer to this plan as the emergency plan or building closure plan. Common scenarios that would lead to the activation of these plans include inclement weather, fire, localized power outages, and localized communications outages. These types of events are generally short-term in nature. SOURCE: FCD 1.

54. **Potential Impact:** The loss of confidentiality, integrity or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets or individuals. SOURCE: FIPS 199.

55. **Primary Mission Essential Functions (PMEFs):** Those MEFs that must be continuously performed to support or implement the uninterrupted performance of NEFs. SOURCE: FCD 1 and 2.

56. **Primary Site:** The location where the primary processing and storage of an IS occurs on a day-to-day basis.

57. **Privacy Posture:** The privacy posture represents the status of the ISs and information resources (e.g., personnel, equipment, funds and information technology) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to comply with applicable privacy requirements and manage privacy risks and to react as the situation changes. SOURCE: NIST SP 800-37.

58. **Reciprocity:** Agreement among participating organizations to accept each other's security assessments to reuse system resources and/or to accept each other's assessed security posture to share information. SOURCE: NIST SP 800-37.

59. **Reconstitution:** The process by which surviving and/or replacement organization personnel resume normal operations. SOURCE: FCD 1.

60. **Recovery:** The implementation of prioritized actions required to return an organization's processes and support functions to operational stability following a change in normal operations. SOURCE: FCD 1.

61. **Recovery Point Objective (RPO):** The point in time to which data must be recovered after an outage. SOURCE: NIST SP 800-34.

62. **Recovery Time Objective (RTO**): The overall length of time an IS's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes. SOURCE: NIST SP 800-34.

63. **Redundancy:** The state of having duplicate capabilities, such as systems, equipment, or resources. SOURCE: FCD 1.

64. **Risk:** The potential for an unwanted outcome resulting from an incident, event or occurrence, as determined by its likelihood and the associated consequences, i.e., the level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. With respect to continuity, risk may degrade or hinder the performance of essential functions and affect critical assets associated with continuity operations. SOURCE: NIST SP 800-18.

65. **Risk Assessment:** The process of identifying risks to agency operations (including mission, functions, image or reputation), agency assets or individuals by determining the probability of occurrence, the resulting impact and additional security controls that would mitigate this impact. Risk assessment is part of risk management, synonymous with risk analysis and incorporates threat and vulnerability analyses. SOURCE: NIST SP 800-18.

66. **Risk Management:** The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets or individuals resulting from the operation of an IS. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency,

and constraints due to laws, directives, policies or regulations. SOURCE: NIST SP 800-18.

67. **Safeguards:** Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity and availability) specified for an IS. Safeguards may include security features, management constraints, personnel security; and security of physical structures, areas, and devices. Safeguards are synonymous with security controls and countermeasures. SOURCE: NIST SP 800-18.

68. **Scenario:** A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives. SOURCE: NIST SP 800-84.

69. **Security Categorization:** The process of determining the security category for information or a system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See security category below. SOURCE: FIPS 199.

70. **Security Category:** The characterization of information or an IS based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or IS would have on organizational operations, organizational assets or individuals. SOURCE: FIPS 199.

71. **Security Controls:** The management, operational, and technical controls prescribed for an IS to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: FIPS 199.

72. **Security Objective:** Confidentiality, integrity, or availability. SOURCE: FIPS 199.

73. **Security Posture:** The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. Security posture is synonymous with security status. SOURCE: NIST SP 800-37.

74. **Security Requirement:** A requirement levied on an IS or an organization that is derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. Note: security requirements can be used in a variety of contexts, from high-level policy activities to low-level implementation activities, in system development and engineering disciplines. SOURCE: NIST SP 800-37.

75. **Specification:** A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or

component and often the procedures for determining whether these provisions have been satisfied. SOURCE: NIST SP 800-37.

76. **System Component:** A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software and firmware. SOURCE: NIST SP 800-37.

77. **Software Development Life Cycle (SDLC):** The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation, and maintenance and ultimately its disposal that instigates another system initiation. SOURCE: NIST SP 800-34.

78. **System Security Plan (SSP):** A formal document that provides an overview of the security requirements for the IS and describes the security controls in place or planned for meeting those requirements. SOURCE: NIST SP 800-18.

79. **System Test:** A test performed on a complete system to evaluate its compliance with specified requirements. SOURCE: NIST SP 800-84.

80. **System User:** An individual (or system process acting on behalf of an individual), authorized to access a system. SOURCE: NIST SP 800-37.

81. **System Specific Control:** A security or privacy control for an IS that is implemented at the system level and is not inherited by any other IS. SOURCE: NIST SP 800-37.

82. **Tabletop Exercise:** A discussion-based exercise where personnel with roles and responsibilities in a particular ISCP meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. SOURCE: NIST SP 800-84.

83. **Technical Controls**: The security controls (i.e., safeguards or countermeasures) for an IS that are primarily implemented and executed by the IS through mechanisms contained in the hardware, software or firmware components of the system. SOURCE: NIST SP 800-18.

84. **Test:** An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in an ISCP. SOURCE: NIST SP 800-84.

85. **Test Guide:** A document that outlines the steps involved in conducting a test and includes a list of the participants, a list of individuals and groups who might be affected by the test, and procedures for early termination of the test. SOURCE: NIST SP 800-84.

86. **Test Plan:** A document that outlines the specific steps that will be performed for a particular test, including the required logistical items and expected outcome or response for each step. SOURCE: NIST SP 800-84.

87. **Testing, Training, Exercises and Evaluation (TTE&E):** Activities designed to familiarize, impart skills, and ensure viability of continuity plans. TTE&E aids in verifying that an organization's continuity plan can support the continued execution of the organization's essential functions during a continuity event.

88. **Threat:** Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image or reputation), agency assets, or individuals through an IS via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: NIST SP 800-18.

89. **Threat Assessment:** Formal description and evaluation of threat to an IS. SOURCE: NIST SP 800-18.

90. **Vulnerability:** Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Note: The term weakness is synonymous for deficiency. Weakness may result in security and/or privacy risks. SOURCE: NIST SP 800-37.

91. **Vulnerability Assessment:** Systematic examination of an IS to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. SOURCE: NIST SP 800-37.

92. **Work Recovery Time (WRT):** The time it takes for a process or function to become fully operational after the system is recovered. WRT includes all recovery actions after the system is operational which will include data recovery and operational/integrity testing.

APPENDIX B – Acronyms and Abbreviation.

Acronym/ Abbreviation	Definition
AAR	After-Action Report
AO	Authorizing Official
AS IT	Assistant Secretary for Information and Technology
ATO	Authorization to Operate
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BPA	Business Process Analysis
CBP	Critical Business Process
CCI	Control Correlation Identifier
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Plan
CIRP	Cyber Incident Response Plan
CISO	Chief Information Security Officer
CNSSI	Committee on National Security Systems Instruction
CP	Contingency Planning
DAS	Deputy Assistant Secretary
DNS	Domain Name System
DRP	Disaster Recovery Plan
ECC	Enterprise Command Center
ECO	Enterprise Command Operations
EDM	Enterprise Directives Management
eMASS	Enterprise Mission Assurance Support Services
EPR	Emergency Preparedness and Response
ERG	Emergency Relocation Group
ESA	Essential Supporting Activity
FCD	Federal Continuity Directive
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard

Acronym/ Abbreviation	Definition
FISMA	Federal Information Security Modernization Act
GRC	Governance, Risk and Compliance
HVA	High Value Asset
IOC	Integrated Operations Center
IS	Information System
ISA	Interconnection Security Agreement
ISCP	Information System Contingency Plan
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITPI CMA	Information Technology Program Integration Continuity and Mission Assurance
KS	Knowledge Service
LAN	Local Area Network
MA	Mission Assignment
MEF	Mission Essential Function
MOU	Memorandum of Understanding
MTD	Maximum Tolerable Downtime
NAS	Network-Attached Storage
NEF	National Essential Function
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NSP	Network Service Provider
OEM	Office of Emergency Management
OEP	Occupant Emergency Plan
OIS	Office of Information Security
OIT	Office of Information Technology
OMB	Office of Management and Budget
OSP	Operations, Security and Preparedness
PHI	Protected Health Information
PII	Personally Identifiable Information

Acronym/ Abbreviation	Definition
PMEF	Primary Mission Essential Function
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPD	Presidential Policy Directive
RAID	Redundant Array of Independent Disks
RMF	Risk Management Framework
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAN	Storage Area Network
SDLC	System Development Life Cycle
SLA	Service-Level Agreement
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SOR	System of Records
SP	Special Publication
SSP	System Security Plan
TTE&E	Testing, Training, Exercise and Evaluation
U.S.C.	United States Code
VA	Department of Veterans Affairs
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WRT	Work Recovery Time

APPENDIX C - ISCP Development Process.

a. **ISCP Data Collection:** Prior to beginning the ISCP development process, it is essential that the ISCP Coordinator collect key data to support the ISCP. The ISCP Coordinator will work with the various VA Departments to include Pharmacy, Nursing Services, Eligibility Determination, Headstones, and Markers, etc. to understand essential functions, Critical Business Processes (CBPs), threat/vulnerability information, and other ISs that depend on or support the IS. They will work with the ISO/ISSO to identify the IS security impact levels based on the FIPS 199 guidance. The ISO/ISSO should also provide information on whether the IS contains personally identifiable information (PII) and/or protected health information (PHI). This information is critical to the development of the ISCP, and lack of sufficient background research will hamper the development of an effective ISCP.

b. **Essential Functions:** The proper identification of essential functions is critical to the continuity and IS contingency planning processes. The ISCP Coordinator should be strongly aware of them before developing the ISCP. Essential functions are those functions the VA must continue in an emergency, whether the functions are PMEFs, MEFs, or ESAs. It is critical that the ISCP Coordinator collaborates with ITPI CMA and Business Owner to ensure they are aware of the essential functions for the VA and the departments they support. This will be essential in Step 2 of the ISCP planning process and should be clearly defined within the ISCP along with the criticality of the systems that support the essential functions. The MEF identification process is outlined in FCD 2 Annex B. The VA MEFs are outlined in the systems-based BIA template in the VA Knowledge Service.

c. **BPA:** The ISCP Coordinators will work with ITPI CMA and Business Owners to review and understand the CBPs that were identified. A solid understanding of these CBPs will allow the ISCP Coordinator to determine which IS services support them and their corresponding MEFs. This is necessary for conducting the systems-based BIA which will be discussed in the following sections. Examples of IS services that could support the CBPs include telecommunications, data communications, helpdesk, web applications, email, the network, and telephone services. The BPA process is outlined in FCD 2 Annex C.

d. **Threat and Vulnerability Assessments:** During continuity planning, assessments are conducted to identify the threats and vulnerabilities to the IS. Threats will include natural (floods, hurricanes, earthquakes, extreme temperatures, etc.), technical/environmental (diseases, power failures, hazardous material spills, etc.), and human (criminals, terrorist events, user negligence, etc.). The COOP plan should identify the likelihood of these threats occurring. Any IS vulnerabilities that may be exploited by the threats and impact operations should also be considered.

(1) The ISCP Coordinator should work with the continuity planners to understand the threats and vulnerabilities identified for the business processes relevant to their IS. Threats and vulnerabilities will not be used for the systems-based BIA, as it focuses on the impact that losing the IS would have on business processes regardless of the threat/hazard that is responsible.

(2) However, this understanding will help the ISCP Coordinator to identify appropriate contingency strategies to mitigate the impacts to the system. These contingency strategies could include, for example, certain environmental controls that will support the IS during a natural disaster.

e. **Security Objectives:** Under FISMA, ISs should define the security objectives of confidentiality, integrity and availability, with the impact categorization levels of low, moderate, or high. FIPS 199 provides criteria to support selection of impact level for each security objective. The availability security objective serves as a basis of the systems-based BIA and all three objectives will be used to guide contingency strategies and recovery efforts. These impact categorization levels are identified by the ISO/ISSO in the SSP. The ISCP Coordinator should be aware of these security objectives and impact levels as they will affect the systems-based BIA and IS contingency planning strategies for the ISCP development.

f. **System Interconnections:** In addition to the security impact levels, the ISCP Coordinator should work with the ISO/ISSO to identify supporting IS interdependencies such as applications and systems that the IS is either reliant upon or supports. These can be both internal or external connections and local or national connections. This information should be captured within the SSP when identifying the authorization boundaries. This information will be critical in identifying the impacts of system loss as well as the contingency strategies for a response. Applicable external system interconnections must have current documented MOUs/ISAs in place.

g. **PII and PHI:** The ISCP Coordinator should work with the ISO, ISSO, and Privacy Officer to determine whether the system contains PII or PHI, as defined by VA Directive 6502, VA Enterprise Privacy Program. The Privacy Act of 1974 and the Health Insurance Portability and Accountability Act place special requirements on the protection of these types of data. These special protections need to be considered when the ISCP Coordinator develops the ISCP and associated documents.

h. **Process-based BIA vs. Systems-based BIA**: As with continuity and IS contingency planning, there is often confusion between process- and systems-based BIAs. The process-based BIA is conducted first as part of the continuity planning by the Administration/Staff Offices. It is conducted in accordance with FCD 2 and is a five-step process that identifies the threats/hazards to the departmental mission and/or business processes and their associated impacts

to those business processes. After the process-based BIA is conducted, the systems-based BIA can be conducted by the ISCP Coordinator as Step 2 of the IS contingency planning process. Systems-based BIA is a three-part process that will align the impact of an IS outage to the business essential functions identified in the process-based BIA. The systems-based BIA will be the focus for IS contingency planning within this guidance.

i. **Systems-based BIA Process:** There are three parts required to accomplish the systems-based BIA.

(1) **Part 1 - Determine Mission/Business Processes and Recovery Criticality:** An IS can be very complex, and often supports multiple mission/business processes. This can result in different perspectives on the importance of system services or capabilities. ISCP Coordinators should work with the VA Departments to identify and understand the CBPs. They then determine which of the CBPs the IS supports, as well as the MEF(s) to which those CBPs align. These business processes and a description should be captured and defined as shown in the table below.

Table 1: Business Process Descriptions (Example)

Mission/Business Process	VA Department	Description	MEF or PMEF Supported
Pay vendor invoice	VBA	Process of obligating funds, issuing check or electronic payment and acknowledging receipt.	None
Patient admittance and discharge	VHA	Process of documenting and admitting or discharging Veterans for patient care.	Healthcare to Veterans

(2) **Identify Outage Impacts:** Once those CBPs are identified, the impact of a system outage to those processes is determined along with outage impacts and estimated downtime of the IS. The ISCP Coordinator will work with the business/service line respondents to determine and quantify the outage impacts. An outage impact quantifies how a loss or disruption of a given IS service affects the ability of a business/service line to continue performing CBPs over time. Organizational and system uniqueness are important considerations for IS contingency planning and business impact. It is important to define and consistently quantify these impacts across an organization so that the planning is standardized. Impact categories and values unique to the VA have been identified in Table 2 below. ISCP Coordinators may identify additional impact categories as necessary and applicable to their specific IS. Additional information is available in the systems-based BIA template in the VA Knowledge Service.

Table 2: Impact Categories and Values

Impact Values	Financial Loss	Customer Impact	Legal / Regulatory Requirements	Reputation	Impact to other Systems
Severe	Loss of the IS will result in a financial loss of more than 75% of the VA department's annual revenue.	Loss of the IS will result in degradation of medical care or service to more than 75% of the VA department's customers (to include Veterans and VA personnel).	Loss of the IS will result in lack of compliance with one or more Federal guidance.	Loss of the IS will result in 1 or more Congressional inquiries.	Loss of the IS will result in loss of functionality of 1 or more high value asset systems.
Moderate	Loss of the IS will result in a financial loss of 25-75% of the VA department's annual revenue.	Loss of the IS will result in degradation of medical care or service to 25-75% of the VA department's customers (to include Veterans and VA personnel).	Loss of the IS will result in lack of compliance with one or more NIST guidance.	Loss of the IS will result in more than a 10% increase in Help desk tickets and/or inquiries to VA leadership.	Loss of the IS will result in loss of functionality of 1 or more FIPS 199 High Availability systems.
Minimal	Loss of the IS will result in a financial loss of less than 25% of the VA department's annual revenue.	Loss of the IS will result in degradation of medical care or service to less than 25% of the VA department's customers (to include Veterans and VA personnel).	Loss of the IS will result in lack of compliance with one or more VA guidance.	Loss of the IS will result in an increase of less than 10% of Help desk tickets.	Loss of the IS will result in loss of functionality of 1 or more Low or Moderate Availability systems.

(3) **Impact Timeline:** Outage impacts are further defined with the MTD, RTO, RPO, and WRT. The MTD represents the total amount of time the ISO/AO are willing to accept for a mission/business process outage or disruption and includes all impact considerations. The MTD covers the entire timeframe from when the system becomes unavailable via a disruptive event through the recovery time frame until normal operations are resumed. Determining MTD is important because not doing so could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method and (2) the depth of detail which will be required when developing recovery procedures, including their scope and

content. RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. RTO covers the timeframe from when the system becomes unavailable via a disruptive event, when system recovery begins and ends when the system is completely recovered. This does not include the data recovery and system verification operations which are part of the WRT. The WRT is the amount of time it takes the system from the time lost data and work backlogs are recovered until the system resumes normal operations. The WRT also includes testing and verifying the system and its data. If the RTO exceeds the MTD, recovery strategies should be adjusted so that the MTD can be met. However, for operational circumstances where this is not possible, the plan will so state and OIT and the Veterans Health Administration, Veterans Benefits Administration and National Cemetery Administration leadership will be formally notified. Finally, the RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered after an outage, given the most recent backup copy of the data. Unlike RTO and WRT, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process. See Figure 1, Impact Timeline, below to understand the relationship between these items.

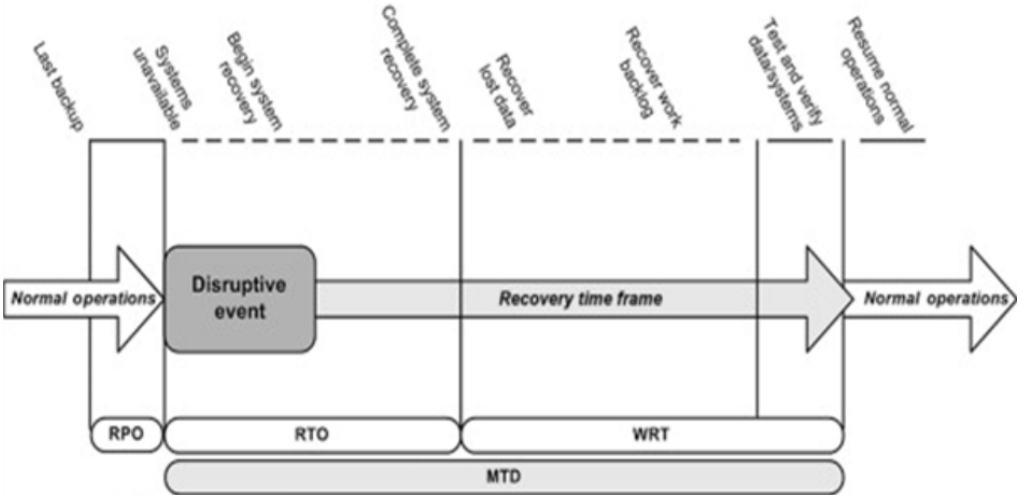

Figure 1: Impact Timeline

(4) **MTD** can vary widely, depending on the technologies employed for recovery, including the point in time from which backup data resources can be recovered and restored. MTD should not be confused with service response time by OIT personnel or vendors. It is expected that the business/service line will have multiple IS services and impacts. The ISCP Coordinator should work with the business/service line respondents to

determine the MTD for IS services. MTDs must correlate with the earliest timeframe that the IS's service outage becomes critical to the mission/business process. MTDs for IS services that support MEFs or are determined to be High Value Assets (HVAs) and HA assets must not exceed twelve hours. It is recommended that MTDs for moderate availability assets not exceed 72 hours and low availability assets should not exceed 30 days. The MTD is established at the point where the potential impact is initially determined to be either moderate or high. For example, a service/business line using a CBP with low impact at 12 hours and high or moderate impact at 72 hours would be assigned an MTD of 72 hours. A moderate or high impact is one that would have a serious (moderate) or severe/catastrophic (high) adverse effect on organizational operations, organizational assets or individuals. Length of MTDs shall be in the following intervals: immediate, 4 Hours, 8 Hours, 12 Hours, 24 Hours, 48 Hours, 72 Hours, 7 Days, 30 Days, and > 30 Days.

(5) **RTO and WRT:** Determining the IS's RTO and WRT is important, as it impacts the selection of appropriate technologies that are best suited for meeting the MTD. The ISCP Coordinator should ensure that the RTO and WRT does not exceed the MTD. For example, a system outage may prevent a particular process from being completed and because it takes time to reprocess the data after the system is recovered, that additional processing time must be considered in the RTO and WRT to stay within the time limit established by the MTD. Once the RTO and WRT is determined, the ISCP Coordinator should determine the MTD - (RTO+WRT) gap for each mission/business process. If MTD is less than RTO+WRT (if MTD - (RTO+WRT) is negative), then this is an issue that the ISCP Coordinator needs to address. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestones should be initiated to document the situation and plan for its mitigation. Mitigation may entail adjustment of recovery strategies and technology.

Table 3: Determine MTD Gap

Mission/Business process with Lowest MTD	MTD	RTO/WRT	GAP (MTD – RTO/WRT)
	Choose an item	Choose an item	

(6) **RPO** should determine the optimum point from which to recover the IS data. When determining this point, VA must consider the criticality of the system and data, the cost of the system being inoperable, or the data being lost and the cost of the resources that are required to restore the system and data. VA must ensure that the backups and alternate storage

and processing sites meet the RPO requirements. A system that requires high integrity of data should have a RPO of less than two hours. A moderate integrity system should have a RPO of less than 24 hours. All this information can be captured visually within the BIA and ISCP to show the relation of the information. An example is shown in Table 4.

Table 4: BIA Information (Example)

Business Process	Potential Impact (Category & Value)	MTD	System Components	RTO	WRT	RPO	Confid.	Integrity	Avail.
Create Budget	Reputation (Severe)	36 hrs.	Database Server	12 hrs.	24 hrs.	12 hrs.	L	M	M
Create Budget	Reputation (Severe)	36 hrs.	Application Server	12 hrs.	24 hrs.	12 hrs.	L	M	M
Process Invoice	Customer Impact (Moderate)	72 hrs.	Application Server	36hrs	24 hrs.	24hrs	L	L	L
Process Invoice	Customer Impact (Moderate)	72 hrs.	Web Server	8hrs	4 hrs.	2hrs	H	M	H

(7) **Part 2 - Identify Resource Requirements:** The ISCP Coordinator will work with the ISO/ISSO to identify all IS components for each IS service hosted in their boundaries. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and essential records. Resources should be identified individually or as a logical group. For a complete list of components, refer to the equipment inventory listing for applicable inventory data such as type of equipment and model information. Equipment inventory, as listed in the GRC tool, should be verified and updated annually. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes as quickly as possible. Working with management and internal and external POCs associated with the system, the ISCP Coordinator should ensure that the complete IS resources are identified. They should further identify any alternate strategies in place to meet expected RTOs. This includes backup or spare equipment and vendor support contracts, as these will impact recovery priorities in the next step.

Table 5: Resource Requirements

System Resource/Component	Platform/Operating System/Version	Description	Alternate Strategies
Application Server	Sun V245/ Solaris / v10.0	Serves as the main application server	Backup server at alternate site

(8) **Part 3 - Identify Recovery Priorities for System:** Based on the results from the previous activities, system resources can be linked more clearly to

critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources. Recovery priorities are established based on dependencies, RTO and PMEF support. Developing recovery priorities is the last step of the systems-based BIA process. Recovery priorities can be effectively established by taking into consideration mission/business process criticality, outage impacts, tolerable downtime, and system resources. The result is an IS recovery priority hierarchy. The ISCP Coordinator should consider system recovery measures and technologies to meet the recovery priorities. Table 6 is an example below. The IS recovery priority hierarchy lists the order of recovery for system components and the expected time for recovering the resource following a worst-case disruption (complete rebuild, repair or replacement).

Table 6: Recovery Priorities (Example)

Priority	System resource/component	RTO
Database	Server	12 hours to rebuild or replace
Storage Files	Isolinear Chip	24 hours to repair or replace
Website	Server	4 hours to repair or replace

j. **Identify Security Controls and Preventive Measures:**

(1) **Security Controls** established in NIST SP 800-53 Revision 5 provide a solid foundation for establishing IS security, integrity and contingency policies. Adherence to these controls for IS contingency planning purposes helps protect an IS against threats that can disrupt operations. VA uses security controls as part of the overall RMF which includes the CP control family. The controls are selected and assigned to each system based on a baseline which is determined by the system's FIPS 199 categorizations (high, moderate, low). VA uses a tiered approach to the implementation and ongoing management of the controls and their underlying Control Correlation Identifiers (CCIs). Determining which parties are responsible for specific requirements is an important part of IS contingency planning. The following are explanations for the three types of control responsibility assignments used by VA:

(a) **System specific controls** and CCI implementations, management and compliance are the sole responsibility of the stakeholders (ISO, System Steward, ISSO) for that system.

(b) **Common controls** and CCI implementations, management, and compliance responsibilities for the system are inherited from another entity within the VA. These entities could include internal or external hosting facilities, area systems that host applications or VA Enterprise entities such as the T1-System of Records (SOR) and IO-SOR.

(c) **Hybrid controls** and CCI implementations, management and compliance are shared between the system and another entity; typically, these are the same entities that would provide inheritance for common controls. Hybrid controls and CCIs can present a challenge for IS contingency planning and strategy. It is important to determine exactly which entities are responsible for each requirement that makes up the entire control. The control documentation describes how system specific and hybrid controls are implemented. It describes the plans and expectations regarding the functionality of the system. The description includes planned inputs, expected behavior and expected outputs where appropriate, typically for those controls implemented in the hardware, software or firmware components of the system. Common controls are also identified in the plans. There is no requirement to provide implementation details for inherited common controls; those details are provided in the plans for common control providers and are made available to appropriate personnel. For hybrid controls, the organization specifies in the system-level plans the parts of the control that are provided by the common control provider and the parts of the control that are implemented at the information system level.

(d) **Identify and Select Controls:** Effective IS contingency planning includes incorporating security controls early in the development of an IS and maintaining these controls on an ongoing basis. Refer to NIST SP 800-53, Revision 5, Chapter 3.6 for security and privacy controls as it relates to CP and the eMASS Implementation Guide for detailed procedures and responsibilities for control selection.

(e) **Implement Controls:** Documentation of planned control implementations allows for traceability of decisions prior to and after the deployment of the system. The documentation must address platform dependencies and include any additional information necessary to describe how the capability required is to be achieved at the level of detail sufficient to support control implementation and assessment. Documentation for control implementations must follow best practices for hardware and software development and for systems security and privacy engineering disciplines and be consistent with established policies and procedures for documenting activities in the SDLC.

(f) **Monitor Controls:** An important aspect of risk management is the ongoing monitoring of controls implemented within or inherited by an IS. An effective continuous monitoring strategy at the information system level is developed and implemented in coordination with the organizational continuous monitoring strategy early in the SDLC. The system-level continuous monitoring strategy, consistent with the organizational monitoring strategy, defines how changes to the

system and the environment of operation are to be monitored; how risk assessments are to be conducted; and the security and privacy posture reporting requirements, including recipients of the reports. The system-level continuous monitoring strategy can be included in security and privacy plans.

(g) **Preventive Measures:** ISs should be built to include preventive measures that attempt to stop an incident before it can occur. The two key parts to this strategy are the concepts of resilience and redundancy.

(2) **Resilience:** Part of a successful IS contingency planning policy is making a system resilient to environmental and component-level failures that would otherwise cause system disruptions. There are several methods for making valuable hardware and software resilient. Determination of the appropriate methods should be based on risk-informed decisions. Depending on results of the risk management process, these methods may or may not be applicable for a particular system.

(3) **Redundancy:** HA is a process where redundancy and failover processes are built into a system to maximize its uptime and availability. The concept of HA is to achieve an uptime of 99.999 percent or higher. Typically, HA technology solutions are used for systems that are categorized as being high (FIPS 199) level systems due to their mission critical business functions and are often considered to be HVAs in the organization. These technologies should be incorporated within the contingency strategies to meet the ISCP planning needs.

(4) **Backups and Recovery for Information and Systems:** Contingency strategies must be designed for data backup for all VA ISs to create a duplicate of data and safeguard it against inadvertent deletion or corruption. The data types to be backed up include user information, system information and security documentation. This might include documents such as contracts, schematics and patient forms, for example. There are many kinds of backups and each one is designed to do a specific job. The primary purpose of a standard backup is to produce copies of data taken from a single system or several systems located across a network. Backups of a system are copies of the system, including all associated configurations and settings.

k. **Security Backup Criteria:** The selected backup methods for the organization will be dependent on several factors:

(1) the frequency at which new data and information sets are introduced to the system;

(2) the availability of the system and data at hand; and

(3) the fulfillment and attainment of the integrity requirements.

(4) Once the backup methods are determined, the ISCP will include backup procedures that will incorporate:

(5) the location where the backed-up data will be stored;

(6) the convention for naming the files and segments;

(7) the rotation frequency of all the media used;

(8) transportation methods for the backup equipment;

(9) the format (how much data it holds, for how long, frequency, categorization, tiers) for:

(a) media types used;

(b) disk drives (solid state or magnetic) including drive arrays (SAN, NAS); and

(c) optical disks.

(10) The frequency of testing the backup information to verify media reliability and information integrity in accordance with requirements defined in the VA Knowledge Service; and

(11) The storage of critical IS software and other security related information in a separate facility or in a fire-rated container not collocated with the operational IS for high category systems.

l. **Recovery Types based on System Categorization:** The backup procedure will be deployed using a differential, incremental or full approach. Both incremental and differential backups pay attention to the differences that occur between versions of data on a system. However, the incremental and differential backups concentrate on distinct aspects of the differences.

(1) **Differential:** Involves only the files that have been changed or added since the most recent full backup was saved.

(2) **Incremental:** Only saves copies of the data in files that have been modified since the last backup, which may have been a full or incremental backup. When comparing the two options, incremental backups are a great deal quicker than differential backups.

(3) **Full:** Full backups are the most basic backup type. This type of backup will back up all the files, folders and partition disks. A full backup is time-consuming and requires significant storage space. Refer to NIST SP 800-

34 Rev. 1 Chapter 3 and 4 for additional information on the ISCP process and development.

m. **Disaster Recovery Plan (DRP)**

(1) **Summary:** The DRP applies to major, usually physical, disruptions to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system-focused plan designed to restore operability of the target system, application or computer facility infrastructure at an alternate site after an emergency. The DRP may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. A DRP may support a BCP or COOP plan by recovering supporting systems for mission/business processes or mission essential functions at an alternate location. The DRP only addresses information system disruptions that require relocation.

n. **DRP Components:**

(1) **Determine recovery objectives** using the information from the systems-based BIA.

(2) **Assign roles and responsibilities for the disaster recovery team:** Create a disaster recovery team that includes a DRP Director and DRP Director (alternate). Assign and document all team member roles and responsibilities in the DRP template.

(3) **Identify an alternate disaster recovery site** for situations when a disaster occurred that severely damaged the primary site, making it impossible to resume operations at the primary site and forcing migration of critical workloads to alternate site. The alternate site will be used for the purpose of emergency relocation of critical data, applications, staff and physical resources. The alternate site must be equipped with appropriate resources in accordance with the FIPS 199 availability level.

(4) **Determine equipment needs:** Conduct an inventory of required office equipment including workstations, laptops, telephones, office furniture, and other accessories. This will help determine how much equipment is required to restore the alternate site infrastructure to an operational state and determine how much equipment is sufficient for supporting mission-critical workloads.

(5) **Detail disaster response procedures:** Develop a disaster recovery checklist which outlines the steps needed to deal with the crisis. Clearly state and document what is expected, and which actions must be taken when disaster strikes.

(6) **Enable communication channels:**

(a) **Internal Communications:** The DRP must provide for processes or equipment to be used in enabling internal communications. Determine which communication channel should be used when the primary site is disabled, and network infrastructure goes down. Staff and management need to know what has occurred, the status of the situation, what actions to take, and who oversees the situation. One person or team must be responsible for internal communication.

(b) **External Communications:** Report the incident to stakeholders. Who to contact, time requirements for contacting, and what must be reported to stakeholders, such as members of the public relations and marketing team, vendors, third-party suppliers, and customers. Also, address how best to inform each of these groups and formulate answers for addressing concerns.

(c) **Test and update the DRP:** Review, test, and update each DRP at least annually to see if there are any inconsistencies and identify what should be improved to achieve the best disaster recovery results.