

NOAA/NESDIS



NESDIS CONTINUITY OF OPERATIONS (COOP) March 2017

COMPLIANCE IS MANDATORY



Prepared by:
U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)



**NESDIS
Policy
Directive**

NESDIS-PD-1070.1
Effective Date: March 3, 2017
Expiration Date: March 2, 2022

THIS PAGE INTENTIONALLY BLANK



Approval Page

Document Number: NESDIS-PD-1070.1 Revision 0.0	
Document Title Block: NESDIS CONTINUITY OF OPERATIONS POLICY DIRECTIVE	
Process Owner:	Document Release Date: March 03, 2017

Prepared by:

WISSMAN.ALPHONSE.J.JR.136
5840810

Digitally signed by WISSMAN.ALPHONSE.JJR.1365840810
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=OTHER, cn=WISSMAN.ALPHONSE.JJR.1365840810
Date: 2017.03.03 08:35:01 -05'00'

Al Wissman
Data Management & Continuity Operations Branch

Date

Approved by:

TIELKING.TERRANCE
E.ALLAN.10194745
22

Digitally signed by
TIELKING.TERRANCE.ALLAN.1019474522
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=OTHER,
cn=TIELKING.TERRANCE.ALLAN.1019474522
Date: 2017.03.03 09:15:48 -05'00'

03/03/2017

Terrance Tielking
Deputy Assistant Chief Information Officer

Date

Irene Parker
Assistant Chief Information Officer

3/7/17

Date

Mark Paese
Deputy Assistant Administrator for Satellite
and Information Services

3/22/17

Date



Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
Rev 0	March 8, 2017	N/A	All	Baseline



Contents

1. Purpose	4
2. Objectives	4
3. Applicability	4
4. Assumptions.....	4
5. Personnel Responsibilities	5
5.1 NOAA Assistant Administrator for Satellite and Information Services.....	5
5.2 Deputy Assistant Administrator/Satellite and Information Services.....	5
5.3 Deputy Assistant Administrator for Systems	5
5.4 NESDIS Office and Data Center Directors	5
5.5 Senior NESDIS Site Personnel	6
5.6 NESDIS COOP Coordinator.....	6
5.7 Personnel Designated as COOP Personnel	7
5.8 Drive-away Kit.....	7
6. Plan Format, Maintenance, and Distribution	7
6.1 Plan Maintenance	7
6.2 Plan Distribution	7
6.3 Directive Effective Date	8
7. Tests, Training, and Exercises (TT&É)	8
APPENDIX A – Authorities.....	9
APPENDIX B – Definitions.....	11
APPENDIX C - Establishing Primary Mission Essential Functions.....	14
APPENDIX D - Developing COOP Plans.....	15
APPENDIX E - Drive-away Kit Checklists.....	19
APPENDIX F - Essential Records.....	21



1. Purpose

This directive establishes policies and procedures for developing and implementing Continuity of Operations (COOP) Plans for the National Environmental Satellite, Data, and Information Service (NESDIS). It describes the roles and responsibilities of key personnel when dealing with incidents or catastrophic emergencies to protect life, preserve equipment, facilities and assets, and restore normal operations.

2. Objectives

Continuity of operations planning is a coordinated effort to ensure a high level of readiness and a capability to implement a plan, with or without warning, to sustain an organization's Mission Essential Functions (MEFs), Primary Mission Essential Functions (PMEFs), and Essential Supporting Activities (ESAs) while protecting the lives of personnel, preserving equipment, and facilities and assets.

NESDIS Continuity of Operations (COOP) planning will ensure:

- Safe and effective protection of all personnel either through evacuation or Shelter-in-Place (SIP)
- Protect and preserve equipment, facilities, and other assets needed to continue MEFs, PMEFS, and ESAs
- Safe and effective staff, resource, and functional relocation to alternate facilities when necessary

3. Applicability

This directive applies to all NESDIS functions, personnel, and designated contractors assigned to or visiting NESDIS offices and data centers.

4. Assumptions

The NESDIS COOP Plan is based on the following assumptions:

1. Incidents and catastrophic emergencies can and will occur at any time and at any NESDIS site or office and data center. In some cases, dissemination of alert and warning and increased readiness measures may be possible. However, many incidents and catastrophic emergencies can and will occur with little or no warning.
2. Outside assistance should be available in most emergency situations affecting a NESDIS site. However, NESDIS personnel should be prepared to carry out initial incident management and short-term actions independently. COOP activation may be required for community-wide disasters impacting a NESDIS site and the surrounding community.
3. Management is responsible for the safety and well-being of personnel and will assume their responsibilities in the implementation of this directive.



4. Implementation of this directive enhances the NESDIS' capabilities to effectively and efficiently prepare for, respond to, recover from, and mitigate all potential hazards, regardless of cause, size, location, or complexity.

5. Personnel Responsibilities

5.1 NOAA Assistant Administrator for Satellite and Information Services

The NOAA Assistant Administrator for Satellite and Information Services will:

1. Direct development, maintenance, and implementation of COOP Plans, including a Business Impact Analysis (BIA) for NESDIS offices and data centers.
2. Direct development, documentation, and implementation of delegations of authority and orders of succession. At least one person in the orders of succession will be located outside of the local geographical area of the facility.
3. Direct development, implementation, and maintenance of a NESDIS Essential Records Program for NESDIS offices and data centers.
4. Direct development, documentation, and maintenance of interagency agreements unique to a particular office necessary to sustain critical infrastructure or an essential function.
5. Ensure adequate equipment, procedures, reports, plans, publications, and other essential records as necessary to sustain essential functions are available at alternate locations and devolution facilities.
6. Function as the NESDIS Incident Commander (IC) of the NESDIS Crisis Management Team (CMT), unless directed to deploy to NOAA's alternate site.

5.2 Deputy Assistant Administrator/Satellite and Information Services

The Deputy Assistant Administrator for Satellite and Information Services will:

1. Assist the Assistant Administrator in the execution of all duties related to COOP
2. Assume all duties of the Assistant Administrator in the absence of the Assistant Administrator

5.3 Deputy Assistant Administrator for Systems

The Deputy Assistant Administrator for Systems will:

1. Assist the Assistant Administrator in the execution of all duties
2. Assume all duties of the Assistant Administrator in the absence of the Assistant Administrator and the Deputy Assistant Administrator for Satellite and Information Services

5.4 NESDIS Office and Data Center Directors

Office and Data Center Directors will:

1. Develop and maintain COOP Plans, including a BIA, for their offices and data



centers

2. Ensure the COOP plans for their office or data center are consistent with the NESDIS COOP Plan
3. Develop, maintain, and exercise emergency contact lists for their offices and data centers
4. Develop, implement, maintain, and exercise functional backup and personnel cross-training for all PMEFs and MEFs
5. Develop, document, and implement delegations of authority and orders of succession. At least one person in the orders of succession will be located outside of the local geographical area of the office or data center
6. Develop, document, and maintain interagency agreements unique to a particular office necessary to sustain critical infrastructure or an essential function
7. Develop, implement, and maintain an essential records program as part of a Document Management program.

5.5 Senior NESDIS Site Personnel

The Senior NESDIS person at each NESDIS site will:

1. Ensure each office or data center at that site has an approved COOP plan, and all systems for that site have an Information System Contingency Plan (ISCP)
2. Act as the Site Coordinator for their site during all COOP activations; coordinate all COOP activities initiated by other NESDIS offices/data center collocated at the same site
3. Ensure implementation of safety procedures, such as evacuation and shelter-in-place, as outlined in the Occupant Emergency Plan (OEP)

5.6 NESDIS COOP Coordinator

The NESDIS COOP Coordinator and staff will:

1. Support NESDIS leadership in COOP program implementation and during COOP activations
2. Provide COOP technical guidance to all NESDIS offices and data centers including assistance in conducting a BIA and other assessments as necessary
3. Recommend and review COOP planning and recovery strategies for NESDIS offices and data centers to ensure optimum use of resources, based on actual incidents, exercises, and lessons learned
4. Prepare a Multi-Year Program and Strategy Plan (MYPSP) including a program budget sufficient to support a viable NESDIS COOP capability conforming to the planning assumptions and objectives of this directive
5. Develop and conduct exercises and training to support COOP Plan implementation
6. Coordinate with the NOAA Homeland Security Program Office (HSPO) for government-wide, DOC, and NOAA initiated COOP activities
7. Maintain the NESDIS COOP Plan, including BIA for NESDIS HQ



5.7 Personnel Designated as COOP Personnel

All personnel assigned to any COOP organization, group, or team will receive a written designation document, known as the COOP letter, confirming their COOP duties.

All personnel so designated will:

1. Understand their assignment and associated roles and responsibilities
2. Attend scheduled COOP training
3. Participate in all COOP exercises when directed
4. Ensure their supervisor, or team leader have their most current contact information
5. Assume their COOP role during COOP activation
6. Notify team leaders or other authorities of unsafe situations or other conditions that warrant changes to the COOP Plan
7. Maintain a "drive-away kit," if applicable

5.8 Drive-away Kit

At a minimum, each drive-away kit will contain those items a member considers essential to support operations at an alternate site for at least 30 days or until normal operations are resumed. See Appendix E for detailed suggestions for drive-away kit contents.

6. Plan Format, Maintenance, and Distribution

COOP Plans will be reflective of the mission essential functions, primary mission essential functions, and essential supporting activities of the office or data center. Appendix D provides a list of recommended sections and appendices; not all sections and appendices are applicable to all offices and data centers.

6.1 Plan Maintenance

COOP Plans will be reviewed and updated as necessary at least annually and within 30 days of a change of the person in charge of an office/data center. All Plans will be signed by the Plan Owner. An updated COOP Plan will be provided to the NESDIS COOP Program staff no later than 30 days following the annual review.

6.2 Plan Distribution

NESDIS Office and Data Center (O/DC) COOP Plans will be distributed to all personnel with COOP responsibilities. NESDIS and O/DC COOP Plans contain information that may be exempt from mandatory release to the public under the Freedom of Information Act (5 U.S.C. § 552); therefore, they will be handled and safeguarded to prevent unauthorized disclosure. The document will not be released without the prior authorization of the NESDIS or O/DC COOP Coordinator to anyone who does not have a valid "need-to-know" based upon their responsibilities under the NOAA Environmental Satellite, Data, and Information Service Continuity of Operations Plan. When unattended, the document will be protected against theft, compromise, inadvertent access, and unauthorized disclosure.



6.3 Directive Effective Date

This directive is effective as of and upon signature of the Deputy Assistant Administrator for Satellite and Information Services. Further questions about the intent and content should be directed to the NESDIS COOP staff.

7. Tests, Training, and Exercises (TT&E)

A Test, Training, and Exercise program prepares, validates, and familiarizes personnel with an organization's COOP Plan. The NESDIS TT&E Program will comply with the DHS Homeland Security Exercise Evaluation Program (HSEEP). All offices and data centers will, with the assistance and advice of the NESDIS COOP staff, plan, conduct, and document periodic training, testing, and exercises. Additionally, all offices and data centers will participate in an annual NESDIS-wide exercise.

Tests, Training, and Exercises for all NESDIS offices and data centers will include, but are not limited to:

- Awareness and role-based training
- Annual functional exercise of the offices/data centers COOP Plans
- Semi-annual test of office/data center call-down /notification tree
- Quarterly communications tests between:
 - Primary and alternate sites
 - Alternate sites and key partners (as defined by the offices/data centers COOP plans)

Training records and tests/exercise results, together with any supporting documentation, will be forwarded to the NESDIS COOP Coordinator within 30 days of the completion of the tests, training, or exercises. These records will help satisfy both the NESDIS and the NOAA/Homeland Security Program Office's TT&E requirement.



APPENDIX A - Authorities

The Assistant Administrator for Satellite and Information Services directs the procedures contained in this plan under the authority granted by 15 USC, and the following orders and directives:

- 5 U.S.C. Part III, § 6501, Telework Enhancement Act of 2010
- 6 U.S.C § 101 et seq., § 314(a) (15), Homeland Security Act of 2002
- 44 USC § 3101, Records Management by Federal Agencies, January 5, 2009
- 44 USC § 3544(b) (8) Federal Information Security Management Act (FISMA), January 2002
- 51 U.S.C. § 60101, et seq., National and Commercial Space Program Act, December 18, 2010
- 36 CFR § 1223.1 et seq., Electronic Records Management, revised July 1, 2000
- 36 CFR § 1236, Electronic Records Management, revised as of July 1, 2000
- 41 CFR § 101.20.103-4, Occupant Emergency Program, revised as of July 1, 2000
- Executive Order (EO) 12472, Assignment of National Security and Emergency Preparedness Communications Functions, July 6, 2012
- EO 12656, Assignment of Emergency Preparedness Responsibilities, November 18, 1988, as amended
- EO 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001
- EO 13618, Assignment of National Security and Emergency Preparedness Telecommunications Functions, July 6, 2012
- Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements, October 2012
- FCD 2, Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process, July 2013
- Presidential Policy Directive (PPD) – 8, National Preparedness, March 30, 2011 (formerly HSPD-8)
- Presidential Decision Directive (PDD) 39, U.S. Policy on Counter-Terrorism, June 21, 1995
- PDD - 63, Critical Infrastructure Protection (CIP), May 22, 1998
- H.R. 1722 § 6504(d) (2), Continuity of Operations Plans Supersede Telework Policy, January 5, 2010
- Homeland Security Presidential Directive (HSPD) – 3, Homeland Security Advisory System, March 11, 2002
- HSPD – 5, Management of Domestic Incident, February 28, 2003
- HSPD – 7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003
- National Security Presidential Directive 51 (NSPD - 51)/Homeland Security Presidential Directive 20 (HSPD – 20), National Continuity Policy, May 4, 2007



**NESDIS
Policy
Directive**

NESDIS-PD-1070.1
Effective Date: March 3, 2017
Expiration Date: March 2, 2022

-
- National Communications System Directive (NCSD) 3-10, Minimum Requirements for Continuity Communications Capabilities
 - National Communications System Manual (NCSM) 3-10-1, Guidance for Implementing NCSD 3-10 (FOUO), February 26, 2008
 - National Infrastructure Protection Plan, 2013
 - Office of Personnel Management (OPM) Washington, DC Area Dismissal and Closure Procedures, December 2015
 - Office of Management and Budget Circular, A-130 Revised, Appendix III, Security of Federal Automated Information Resources, November 28, 2000
 - Department of Commerce, Administrative Order (DAO) 210-1, Emergency Readiness for Departmental Continuity, November 4, 2009
 - DOC DAO 210-7, Commerce Responsibilities in Disasters, April 15, 1977
 - DOC Telework Policy, October 2014
 - *Vital Records and Records Disaster Mitigation and Recovery, National Archives and Records Administration Instructional Guide Series*, College Park, MD (1996)
 - National Institute of Technology (NIST), Special Publication 800-34 (revision 1), Contingency Planning for Information Technology Systems, May 2010
 - NOAA Administrative Order (NAO) 210-2, Vital Records Program, June 13, 2006
 - NAO 210-5, Order of Succession to Key NOAA Positions, May 14, 2012
 - NAO 210-100, All Hazards Incident Management, January 22, 2014



APPENDIX B - Definitions

Continuity of Government (COG). A coordinated effort within the Federal government's executive branch to ensure that NEFs continue to be performed during a catastrophic emergency.

Continuity of Operations (COOP). A coordinated effort to ensure that Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs) will continue to be performed during a wide range of emergencies, disruptive incidents, or situations focused on, or a threat to, the organization, its personnel or its facilities, including localized acts of nature, accidents, and technological or attack-related emergencies.¹

Continuity of Operations (COOP) Plans. A Continuity of Operations Plan is a critical part of an organization's emergency response planning and contributes significantly to organizational resilience. COOP Plans are part of a suite of plans that organizations develop for emergency response and organizational resilience that can also include: Business Continuity Plans (BCP), Crisis Communications Plans (CCP), Critical Infrastructure Protection Plans (CIPP), Cyber Incident Response Plan (CIRP), Disaster Recovery Plan (DRP), Information System Contingency Plan (ISCP), and Occupant Emergency Plan (OEP). The COOP plan takes an agency-wide view and incorporates many of the aspects of these other plans to create a unified Continuity of Operations approach for NESDIS. COOP Plans are frequently confused with Information System Contingency Plans (ISCPs).

Continuity of Government Readiness Conditions (COGCON). Readiness levels that provide the Executive Branch of the Federal Government with a graduated matrix of protective actions to safeguard personnel, facilities, or operations to ensure continuity of essential operations when the threat level rises². The COGCON matrix consists of four levels ranging from Low Threat (COGCON 4) to High Threat (COGCON 1). The matrix provides guidance to maintain an appropriate level of readiness and operational capability at each phase of the threat to standardize deployment procedures. The President will determine and issue the COGCON Level, and officials and managers of the Executive Branch of the Federal Government will comply with the requirements and assigned responsibilities under the COGCON program.

Emergency. Any situation or condition when a facility is subjected to a bomb or bomb threat, significant civil disturbance, terrorist assault, fire, explosion, major electrical or systems failure, significant chemical spill, gas leak, massive medical trauma, hurricane, tornado, flood, earthquake, or any other similar disabling situation.

¹ FCD 1, Annex P, October 2012

² Ibid



Emergency Relocation Group (ERG). A carefully selected and appointed group of COOP emergency employees assigned the responsibility to report to a continuity site, as required. ERG personnel must have the requisite knowledge, skills, and abilities to perform and continue the mission essential functions of the organization, or other COOP related operations, during any crisis or emergency requiring activation of the COOP plan.

Enduring Constitutional Government (ECG). A cooperative effort among the executive, legislative, and judicial branches of the Federal government, coordinated by the President, as a matter of comity with respect to the legislative and judicial branches and with proper respect for the constitutional separation of powers among the branches, to preserve the constitutional framework under which the Nation is governed. ECG ensures the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the NEFs during a catastrophic emergency.

Essential Function. The critical activities performed by organizations, especially after a disruption of normal activities that enable the organization to accomplish its mission and serve its stakeholders. There are four categories of essential functions: NEFs, MEFs, PMEFs, and ESAs.

- **National Essential Function (NEF).** A government function necessary to lead and sustain the nation during a catastrophic emergency. NEFs will be the primary focus of the President and the national leadership during and following any emergency, and, therefore, must be supported by the Executive Branch of the Federal Government continuity capabilities.
- **Mission Essential Function (MEF).** Essential functions of the Executive Branch of the Federal Government that must be continued throughout or resumed rapidly after a disruption of normal activities. Once identified, MEFs serve as key continuity planning factors for the Executive Branch of the Federal Government organizational elements to determine appropriate staffing, communications, information, facilities, training, and other continuity requirements.
- **Primary Mission Essential Function (PMEF).** Those MEFs that directly support NEFs. PMEFs must be performed by the Executive Branch of the Federal Government to support or maintain NEFs before, during, and after an emergency. Generally, PMEFs must be uninterrupted, or if interrupted, then resumed within the first 12 hours after the occurrence of an emergency and maintained for up to 30 days or until full resumption of normal operations.
- **Essential Supporting Activities (ESAs).** ESAs are critical functions an organization must continue during continuity activation, but that do not meet the threshold for MEFs or PMEFs (e.g. human resources management, security, and facilities management) as candidates for restoration as resources permit.

Essential Records. Records essential to the continued functioning or reconstitution of the Department and its operating units during and after an emergency. Essential records are divided into two categories:



- Emergency operating records include emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical Department and operating unit functions, as well as related policy or procedural records that would be needed to conduct operations under emergency conditions and to resume normal operations after the emergency.
- Legal and financial rights records are essential to protect the legal and financial rights of the government and of the individuals directly affected by its activities. Examples of these records include titles, deeds, leases, contracts, personnel files, and similar records.

Information System Contingency Plans (ISCP). An ISCP is an integral part of a facility COOP Plan and focuses on responding to and recovering operations of a designated information system from an incident or disruption of service and is based on the *Federal Information Security Act of 2002 (FISMA)*.

Occupant Emergency Plan (OEP). A site-specific plan that provides guidance to designated officials and occupants in facilities to protect life, ensure safety, and reduce the risk to personnel, property, and other assets in the event of an emergency either inside or immediately surrounding the facility. The potential exists for any OEP-related emergency to be elevated to a continuity scenario. Managers should always plan for the possibility a COOP plan will be activated during an OEP-related emergency.

Preparedness. The range of plans, policies, procedures, activities, training, and equipment necessary to build, sustain, and improve the operational capabilities to prevent, protect against, respond to, and recover from an emergency. Preparedness is a continuous process involving efforts to identify threats, determine vulnerabilities, and identify required resources to reduce the risk to personnel, facilities, systems, or operations.

Records Management. The identification, protection, and accessibility of identified vital records, databases, and supporting information systems necessary to perform MEFs and PMEFs. Vital records management must be conducted in accordance with FCD 1, Annex I, Vital Records Management; DAO 205-1, Records Management; and the Department's Records Management Policy.



APPENDIX C - Establishing Primary Mission Essential Functions

Among the four Department of Commerce PMEFs, two are designated for NOAA:

DOC PMEF #2 - "Collect and provide the Nation with critical intelligence data, imagery, and other essential information for predictive environmental and atmospheric modeling systems and space-based distress alert systems by operating NOAA-controlled satellites, communications equipment, and associated systems."

DOC PMEF #3 - "Provide the Nation with forecasts, warnings, environmental data, and expertise critical to public safety, disaster preparedness, all-hazards response and recovery, the national transportation system, safe navigation, and the protection of the Nation's critical infrastructure and natural resources."

The following NESDIS PMEFs support the NOAA PMEFs:

1. Satellite command and control critical to retrieve environmental satellite data used for public safety and national security. Communications capabilities to the satellites must be up and running at all times.
2. Ingest, process, and distribute global environmental data and information services from satellites and other sources to promote, protect, and enhance the Nation's economy, security, and the environment.
3. Recover distress signals from geostationary and polar orbiting satellites and distribute them to search and rescue authorities.
4. Implement, as necessary, control over NOAA-licensed private remote sensing space systems' distribution of data for national security reasons (aka implementation of modified operations).



APPENDIX D - Developing COOP Plans

NESDIS HQ and all offices and data centers will use the following procedures to develop, implement, and maintain COOP Plans. Given the difference in missions amongst NESDIS offices, these instructions are written to the highest level. Facilities may modify these instructions as necessary to fit mission and size.

D.1 Business Impact Analysis

The initial step in developing a COOP Plan is accomplishing a Business Impact Analysis. A BIA is a systematic process to identify all business functions, resources to perform those functions and characterize consequences of their loss.

The BIA –

- Identifies all functions and services performed
- The recovery time objective (RTO) of each function
- Associated recovery requirements

The BIA establishes continuity requirements and prioritizes functional recovery based on the RTO. RTOs consider the point at which the loss of a function becomes unacceptable to the organization and are used to help determine the need for COOP activation³.

A BIA will be conducted within 12 months of the date of this Directive and reviewed jointly by the senior leadership at each office/data center and NESDIS COOP program staff, and updated annually not later than December 31 of each year, or within 30 days of a new director assuming responsibility for the office/data center.

D.2 COOP Plan Development

Upon approval of the BIA by the office/data centers director, the office/data center COOP staff, with the assistance of the NESDIS COOP staff, will:

- Identify recovery strategies meeting the approved requirements
- Determine advantages and disadvantages of each recovery strategy
- Implementation recommendations based on cost-effectiveness and the ability to satisfy requirements

A COOP Plan will provide the procedures and support policies necessary to implement the approved strategies. The required elements of the COOP plan will be covered in the following sections.

D.3 Planning Assumptions

It is not possible to predict every eventuality that could require activation of NESDIS COOP plans. All NESDIS facilities are potentially vulnerable to a broad range of accidents, natural disasters, technology or environmental failures, or deliberate acts including war or terrorism.

³ See FCD 2 and NIST SP 800-34, Rev. 1 for guidance in conducting a Business Impact Analysis.



In order to establish baseline planning factors, assumptions will provide initial planning standards. Additional planning assumptions may be necessary for specific facilities and/or locations beyond those listed here.

COOP plans should address, at least, the following:

- All-hazards planning can be addressed if strategies for the following four impacts are adequately developed and implemented:
 1. Loss of computing infrastructure (e.g. hardware/software failure, virus, etc.)
 2. Loss of telecommunications (voice and/or data)
 3. Loss of Personnel
 4. Denial of facility access
- Activation of the COOP plan may result from localized conditions that have little broader impact, a regional situation, or a catastrophic event that severely taxes the ability of the Federal Government to maintain operations.
- NESDIS personnel will be prepared to address any hazard, all conditions and impacts for emergency response, and recovery of MEFs and PMEFs based on predetermined and approved prioritization.
- Assume activation without warning
 1. National guidance requires all executive departments and agencies to base continuity planning on the assumption that advance warning will not be received to implement COOP and shift operations to the alternate site.
 2. COOP procedures may be activated during normal hours as well as non-duty hours.
- Assume Constrained Resources
 1. COOP operations will be conducted with limited staff and technological resources and reduced logistic support aimed at supporting only the most critical NESDIS functions.

D.4 Plan Elements

COOP Plans, as a minimum, will contain the following elements⁴:

1. Essential Functions
 - Define MEFs, PMEFs, and ESAs performed or supported
2. Delegations of authority & succession planning
 - A fully coordinated and approved plan for Orders of Succession and Delegations of Authority
3. COOP Plan activation criteria & procedures
 - Procedures for employee advisories, alerts, formation of the COOP Recovery Organization, and implementation of COOP procedures with instructions for relocation to the appropriate alternate site when necessary

⁴ As outlined in FCD-1



-
- Procedures will support activation, with and without warning, during duty and non-duty hours
 - Maintain up-to-date Fan-out List, Emergency Alert Trees, telephone trees, etc.
4. Alternate facilities
 - A list of alternate locations that are prepared to accommodate migrating functions, services, and staff, including directions, points of contact, and telephone numbers
 - A list of essential services in the immediate vicinity of each identified alternate site, e.g., hospitals and critical care facilities, eating establishments, hotels/motels, etc.
 - Alternate site security policies and check-in procedures
 - Procedures for recovering PMEFS within appropriate RTOs
 - Processes and procedures to acquire resources necessary to sustain operations for at least 30 days or until normal operations are resumed
 - Methods for maintaining operational logs and detailed records of financial activity during COOP operations
 5. Interoperable communications
 - A list of interoperable communications (e.g. telephone, facsimile, cell and/or satellite telephones) to all NESDIS alternate sites and the alternate sites of all higher authorities, and instructions for contacting each site (this information is also maintained within the NESDIS Essential Records located on the NOAA Essential Records Server)
 6. Essential records and databases
 - A list of essential records, as well as their location and instructions for access and retrieval
 7. Human resources
 - A roster of fully-trained personnel with the authority and skills to perform essential functions and activities
 - Procedure for personnel accountability throughout the duration of the COOP event
 - Designation of personnel to the recovery organization structure
 8. Devolution (NESDIS HQ only)
 - Identify a devolution site and designate a Devolution Director
 - Office/data center directors (or designees) work with the Devolution site personnel to identify critical functions to be conducted
 - When activated, the Devolution Director leads the team of staff to support those HQ functions pre-identified until the designated responsibilities are reconstituted
 9. Reconstitution
 - For large-scale reconstitution efforts, a reconstitution plan is required to detail the restoration recommendations, projected costs, and timeline. The reconstitution plan



will be approved by NESDIS leadership

- Procedures for validation testing
- Migration plan (in phases) for returning operations

10. Tests, Training & Exercises

- Guidance for regular COOP testing, training, and exercising

D.5 Notice of Confidentiality

All COOP Plans containing Personally Identifiable Information (PII) will be stored and communicated using accepted PII controls as directed by Department of Commerce, NOAA, and NESDIS policies, directives, and, orders.

All COOP Plans will include the following Notice of Confidentiality, and afforded protections commensurate with "For Official Use Only" (FOUO) information:

"Information contained in this Continuity of Operations Plan (COOP) is FOR OFFICIAL USE ONLY. Portions of this plan may contain information raising privacy or other considerations, which may be exempt from mandatory disclosure under the Freedom of Information Act. The information contained herein is to be used by personnel with an official "Need to Know" based on their responsibilities relative to this COOP activities. Some of the information in this plan, if made public, could endanger the lives and privacy of associates. In addition, the disclosure of information in this plan could compromise the security of essential equipment, services, and systems of the National Environmental Satellite, Data, and Information Service, or otherwise, impact NESDIS' ability to perform its critical functions, as well as disclose protected Personally Identifiable Information (PII). Unauthorized use of this information may constitute an invasion of privacy and a violation of law. When unattended, the document must be stored in a locked container or area offering sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure."



APPENDIX E - Drive-away Kit Checklists

A drive-away kit is a package containing personal and professional items and equipment related to an emergency operation that all Leadership Response Group (LRG) and Emergency Relocation Group (ERG) members should be able to retrieve quickly at all times in case of COOP activation.

E.1 Business Drive-away Kit Checklist

- CAC card
- Directions to alternate facility
- COOP Plans (including individual checklists)
- Government-issued communication equipment
 - Smartphone/cell phone
 - Chargers/batteries for portable communication equipment
 - GETS / WPS card, if issued
 - Satellite phone, if issued
- Laptop/iPad (with accessories, plugins, extra batteries, CAC card readers, chargers, etc.)
- Government credit cards
- Contact information for key personnel and organizations
- Hard copies and/or electronic versions of essential records
- Flashlight w/extra batteries

E.2 Personal Drive-away Kit Checklist

- Personal cell phone/smart phone including chargers
- Identification and credit and debit cards
- Driver's license
- Health insurance card
- Insurance information
- Medical Needs
 - List of allergies/blood type and/or other medical conditions
 - Hearing aids and extra batteries
 - Glasses and/or contact lenses
 - Prescription drugs (minimum 30-day supply)
 - Hard copy of prescriptions
 - Over-the-counter medications, dietary supplements, etc. (minimum 30-day supply)
 - Medical devices
- Emergency Phone Numbers and Addresses (Relatives, Doctors, Pharmacist)
- Postage stamps and personal stationery
- Family Emergency Plan (www.Ready.gov)



-
- Cash for miscellaneous expenses, including coins for vending machines
 - Bottled water and non-perishable food (i.e., granola, dried fruit, etc.)
 - Recreation/entertainment (reading materials, playing cards, puzzles, games)
 - Sewing Kit
 - Flashlight and batteries
 - Trash bags
 - Laundry bag
 - Personal pictures
 - Spiritual materials
 - Lighter/matches
 - Toiletries
 - Toothbrush, toothpaste, dental floss
 - Bath soap
 - Shampoo
 - Hair brush and comb
 - Hair dryer, curling iron
 - Electric razor or razor and shaving cream
 - Nail clippers and file
 - Deodorant or antiperspirant
 - Personal hygiene products
 - Clothing
 - Business casual work attire (4-5 days' worth)
 - Leisure clothes (workout clothing, etc.)
 - Underwear and socks, sleepwear, robe, slippers
 - Light- and medium-weight sweater or jacket
 - Outerwear for the season
 - Comfortable shoes
 - Small portable battery operated radio/CD player/alarm clock

Personnel should add or deduct from this list according to their special needs and operating environment. The drive-away kit should be updated on a regular basis. Any kit containing sensitive and classified documents must be handled and protected in accordance with guidance issued by the DOC Office of Security and requisite federal security guidelines.



APPENDIX F - Essential Records

F.1 Objective

A robust Essential Records Program will provide NESDIS with the records needed to conduct its mission essential and primary mission essential functions under other than normal operating conditions for a minimum of 30-days; and, to resume normal business following an unplanned interruption of operations. In addition, an Essential Records Program will enable NESDIS officials to identify and protect the most important records dealing with the legal and financial rights of the US Government and the agency and of persons directly affected by the agency's actions.

A document's designation as a permanent record has no bearing on its designation as an essential record.

F.2 Responsibilities

1. The NOAA Assistant Administrator for Satellite and Information Services will:
 - Direct development, implementation, and maintenance of an Essential Records Program for NESDIS offices and data centers.
2. Office and Data Center Directors will, with the advice and assistance of the NESDIS COOP staff:
 - Develop and implement an Essential Records Program for their offices and data centers.
 - Appoint an Essential Records Manager for their office or data center.
 - Ensure adequate equipment, procedures, reports, plans, publications, and other essential records necessary to sustain mission essential and primary mission essential functions are available at alternate locations and devolution site.
3. Essential Records Managers will:
 - Understand their assignment and associated roles and responsibilities
 - Ensure their supervisor and ERG team leader have their most current contact information.
 - Ensure a copy, either in electronic form or hard copy, of all essential records is available at all alternate locations and the devolution site (if applicable).
 - Prepare an inventory of the essential records necessary for the office or data center to continue mission essential and primary mission essential functions at alternate and devolution sites for at least 30-days. A copy of this inventory will be provided to the NESDIS COOP Coordinator.
 - Coordinate with the office and Data Center directors to ensure appropriate resources are available at the alternate locations and devolution sites to access the essential records.
4. The NESDIS COOP Coordinator and staff will:



**NESDIS
Policy
Directive**

NESDIS-PD-1070.1
Effective Date: March 3, 2017
Expiration Date: March 2, 2022

-
- Provide advice and direction as required to maintain a NESDIS Essential Records Program.
 - **Maintain access requirements and inventories of resources necessary to access the essential records (hardware, software, Internet access, etc.) at alternate and devolution sites.**
 - Coordinate with the NOAA Homeland Security Program Office (HSPO) for government-wide, DOC, and NOAA essential records activities.



F.3 Essential Records Maintenance

The Essential Records inventory will be reviewed at least annually, no later than December 31 of each year, and within 30 days of a change of the person in charge of an office or data center. Copies of the inventory will be provided to the NESDIS COOP Program staff no later than 30 days following a review.

F.4 Sample Essential Records

1. Emergency-operating Records

- Emergency plans and directive(s), or other authorizing issuances, including information needed to operate the alternate operations center and its equipment, and records recovery plans and procedures
- Orders of succession
- Delegations of authority
- Emergency staffing assignments, including lists of personnel, along with their addresses and telephone numbers (and comparable data for alternates), assigned to the alternate operations center or other emergency duties or authorized access to damaged facilities to assess the extent of damage
- Alternate operations center access credentials and classified or restricted access container documentation (as required)
- List of credit card holders and limits
- Building plans and building systems operations manuals for all agency facilities
- Equipment inventories for agency facilities
- File plans describing the records series and electronic information systems maintained at official filing stations for all agency facilities
- Essential records inventories
- Copies of agency program records (whatever the media) needed to carry out continuing critical functions
- System documentation for any electronic information systems designated as emergency operating records.

2. Records needed to Protect Rights:

- Accounts-receivable records
- Social security records
- Payroll records
- Retirement records
- Insurance records
- Any records relating to contracts, entitlement, titles, deeds or leases, or obligations whose loss would pose a significant risk to the legal and financial rights of the Federal Government or persons directly affected by its actions
- System documentation for any electronic information systems designated as records needed to protect rights.



**NESDIS
Policy
Directive**

NESDIS-PD-1070.1
Effective Date: March 3, 2017
Expiration Date: March 2, 2022



F.5 Essential Records Inventory Requirements

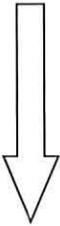
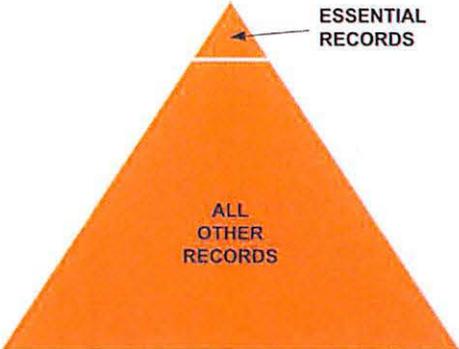
NESDIS offices/data centers are responsible for reviewing their list of essential records annually. Any changes will be updated in the Essential Records Inventory file. In addition to listing the essential records, the file also contains other important information (see table below) related to the records.

Column Heading	Description
Mission Essential Functions, Supporting Activities, and Capabilities	Name the function(s) that requires the essential records (files)
Vital Records	Describe the records (e.g COOP Plan)
Record Series from NOAA Records Management Handbook	If applicable; otherwise leave blank
Location	Provide name of the primary facility where essential records are stored (e.g. SSMC1), provide floor/room number (if known)
Offsite Location	Provide name of the offsite facility (either NESDIS or vendor locations), provide floor/room number (if known)
Media	Hardcopy or electronic, or both
Updates	Frequency of record updates, e.g. weekly, monthly, quarterly, annually
Needed Within	How soon the records are needed during recovery phase, e.g. immediately, X hours, X days
Type	Type of the records, such as Emergency Operations, Financial, and Rights & Interests (contracts)
Emergency Program Contacts -- Local	Essential records POC at the primary site
Emergency Alternate Contacts -- Offsite	Essential records POC at the offsite location



F.7 Prioritization of Essential Records

NOTE: The left-hand column below indicates salvage priorities for essential records based on how quickly access will be required following an emergency.

PRIORITY FOR SALVAGE	ESSENTIAL RECORDS ARE RECORDS THAT:	EXAMPLES INCLUDE:
Priority 1: First 1–12 hours 	Are necessary for emergency response	<ul style="list-style-type: none"> • Copy of emergency and/or Continuity of Operations (COOP) Plan • Infrastructure and utility plans • Maps and building plans • Emergency contact information
	Are necessary to resume or continue operations	<ul style="list-style-type: none"> • Delegations of authority • Contracts and leases • Payroll • Prison, jail, and parole records • Insurance records
Priority 2: First 12–72 hours 	Protect the health, safety, property, and rights of residents	<ul style="list-style-type: none"> • Deeds, mortgages, land records • Birth and marriage records • Medical records • Active court proceedings • Education and military service records • Voting records • Professional licenses
	Would require massive resources to reconstruct	<ul style="list-style-type: none"> • Geographic information systems data • Tax records
Priority 3: After first 72 hours	Document the history of communities and families	<ul style="list-style-type: none"> • Historical documents • Photographs • Identity records
<ul style="list-style-type: none"> • Only a small percentage (typically, less than five percent) of all Government records are essential • Value during an emergency makes a record essential • As disruption time increases, more records become essential • “Records” can be in many different formats, including paper or electronic 		

Source: DHS Records Emergency Planning Essential Records and Response Webinar Handout 2.2 Session 2. Retrieved from https://www.statearchivists.org/files/4214/4476/8338/HO_2-2_Essential_Records_Final_07-2010_508.pdf