Department of Commerce • National Oceanic & Atmospheric Administration • National Weather Service

NATIONAL WEATHER SERVICE POLICY DIRECTIVE 80-3

October 28, 2009

Science and Technology

SYSTEMS ENGINEERING

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: W/OST3 (D. Jones) **Certified by:** W/OST (D. Berchoff)
Type of Issuance: Routine

SUMMARY OF REVISIONS: This directive supersedes NWS Program Directive 80-3, dated April 8, 2004. Changes were made to (1) update Section 1 to add statements to support NOAA and NWS enterprise architecture, NWS mission, and to document system risks and mitigation strategies for sustaining mission goals; (2) update Section 2 to i) include compliance to NOAA and NWS enterprise architecture, ii) include security standards statement, iii) include the System Development Life Cycle (SDLC) security requirements as part of systems engineering framework and add reference to NWSPD 60-7, Information Technology Security Policy, iv) add system maintainability as part of system life cycle requirements, and reference to industry best practices and Federal policies, guidelines, and procedures, v) clarify the enterprise architecture compliance validation and the system requirements validation as two separate tasks, and vi) add relevant references to Acquisition Review Board, Operations and Service Improvement Process, and Change Control Board; (3) add collaboration with the Office of Chief Information Officer for establishing system engineering policies and procedures; (4) update the references of NWS policy directives and instruction, and NIST security publication; (5) update the legal statutory citations for information technology and security.

1. Systems engineering is applied to any system or major program or project and to any lifecycle phase during which design and technical program tasks are defined, evaluated or changed. The National Oceanic Atmospheric Administration (NOAA) National Weather Service (NWS) requires systems engineering functions to support the NOAA and NWS enterprise architecture for both the existing and future NWS mission. In addition, Federal regulations require that all information systems provide adequate protection on data and information, maintain data and software integrity; and that system risks and mitigation strategies be identified and documented for unplanned interruptions in order to sustain mission goals.

2. The objective of this directive is to establish the requirement and framework for systems engineering practices in developing systems and applications in compliance with the NOAA and NWS enterprise architecture. This directive overarches three NWS instructions: 80-303 Systems Engineering for New Development, 80-304 Software Development, and 80-305 Test and Evaluation.

   Systems engineering is an interdisciplinary approach and means to enable the realization of successful systems[1]. Systems engineering uses the following framework:

   a. Systems engineering supports system development, acquisition, program management, operations, and maintenance of mission critical systems to ensure systems are designed, built, operated, and maintained such that they function as needed in a cost-effective and secure way, considering performance, cost, schedule, and risk.

   b. Security standards, operational management, federal enterprise architecture framework, and technical controls will be planned for, designed into, and developed for information systems supporting the mission of NWS.

   c. System functional and performance requirements will be developed from operational requirements as defined through the NWS Policy Directive 10-1, NWS Requirements, Operations and Services Improvements, and the NWS Instructions, 10-103, Operations and Services Improvement Process Implementation.

   d. Security will be addressed in each System Development Life Cycle (SDLC) phase according to NWSPD 60-7, Information Technology Security Policy, and its corresponding laws and guidance, thus advancing the system application and security requirements together to ensure a balanced approach during development.

   e. Tradeoffs between effectiveness and cost will include consideration of alternative architecture designs. Industry best practices and Federal policies, guidelines, and procedures will be applied to ensure sustainable and supportable systems meet mission, performance, security, maintainability, and quality requirements.

   f. Systems engineering processes will include the evaluation of proposed designs to support system, security, and operational requirements.

   g. Systems will be developed consistent with documented requirements, designs, and operational, maintenance, security, and logistics concepts.

[1] INCOSE, *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, Version 3.0, June 2006

h. System baselines will be coordinated with and evaluated by combined engineering and program management functions to ensure operational requirements and appropriate tradeoffs of cost, schedule, and risk meet system objectives.

i. Developed systems will be integrated into the enterprise architecture and architectural compliance validated.

j. Developed systems will be verified and validated to comply with system requirements.

k. Risk management, traceability of requirements through test, effectiveness measure (metrics), configuration management, quality assurance, and logistics support analyses will be used in the system design process.

l. Alternative methods will be considered for acquisition, deployment, operation, and support of systems. Selected alternatives need to be approved by relevant governing authority or process such as Acquisition Review Board (ARB), Operations and Service Improvement Process (OSIP), or Change Control Board (CCB).

3. This directive establishes the following authorities and responsibilities:

3.1 The Office of Science and Technology will collaborate with the Office of Chief Information Officer (OCIO) to establish NWS policies and procedures for systems engineering.

3.2 Each Office and Region is responsible for ensuring systems engineering is conducted in accordance with this policy.

4. This policy directive is supported by the references and glossary of terms listed in Attachment 1.

signed October 14, 2009
John L. Hayes Date
Assistant Administrator for Weather Services

Attachment 1

REFERENCES AND GLOSSARY OF TERMS

References

NWS Policy Directive 10-1, *NWS Requirements, Operations and Services Improvements*
NWS Instruction 10-103, *Operations and Services Improvement Process Implementation*
NWS Policy Directive 80-1, *Acquisition Program Management*
NWS Instruction 80-303, *Systems Engineering for New Development*
NWS Instruction 80-304, *Software Development*
NWS Instruction 80-305, *Test and Evaluation*
NWS Policy Directive 80-4, *Science and Technology Planning and Programming*
NWS Policy Directive 80-5, *Science Review and Approval*
NWS Policy Directive 60-7, *Information Technology Security Policy*
NOAA Administrative Order 212-13, *Information Technology Security Management*
NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
NIST 800-53, *Recommended Security Controls for Federal Information Systems*
NIST 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*
NIST 800-30, *Risk Management Guide for Information Technology Systems*

Glossary

Enterprise. The aggregate of all functional elements, equipment, and processes which together accomplish a common mission.

Enterprise Architecture. A strategic representation of an organization, which defines its mission and business practices, and the information and technology necessary to perform its mission and support its business practices.

Information Security. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542(b)(1)(A)-(C)]

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., Sec. 3502(8)]

Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. [40 U.S.C., Sec. 11101(6)(A)]

Major Program/Project. Program/Project with total costs in excess of a predetermined threshold is deemed to be major program/project.

Mission Critical System. A system that is essential in the performance of a mission objective that if lost, would cause failure to meet or support the mission objective.

Safeguards. Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system.

System. A system is an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

System Architecture. The arrangement of elements and subsystems and the allocation of functions to them to meet system requirements.

Systems Engineer. An engineer trained and experienced in the field of systems engineering.

Systems Engineering Processes. A logical, systematic set of processes selectively used to accomplish systems engineering tasks.

System Requirements. All necessary functional requirements of a system in terms of technical performance and mission requirements, including verification provisions to assure that all requirements are achieved. Essential physical constraints are included.