The NCP is the name for the overall bundle of products shown below. There is no single product that is the NCP, since it is a compilation of other documents.

OTHER DOCUMENTS (located in the supplemental documentation folder):
- Plan of Action & Milestones (POA&M) Template
- Educational Handout - Overview of Cybersecurity Policies
- Supplemental Forms & Reference (e.g., IRP, Data Handling, etc.)
- Cybersecurity Roles & Responsibilities
- NIST 800-171 & CMMC Scoping Guide
- Educational Posters (How To GRC)
- Data Classification Icons
- Cybersecurity Awareness Training Template

PRIMARY NCP COMPONENTS

MAPPED #s

MAPPED #s

POLICIES & STANDARDS

The CDPP is the best place to start, since this document contains the policies and standards that govern the broader NIST 800-171 and CMMC requirements. The footnotes show what CMMC and NIST 800-171 requirements are addressed.

The CDPP is meant to be centrally-managed by the cybersecurity staff. It is the authoritative source for what is required to be implemented by the organization.

The structure of the CDPP covers what is reasonably required for:
- NIST 800-171 CUI controls
- CMMC 2.0 Levels 1 & 2

PROCEDURES

The CSOP is a catalog of procedures. The CSOP is meant to be de-centralized where stakeholders "cut & paste" the controls they are responsible for and document those procedures as they best see fit (e.g., GRC solution, OneNote, SharePoint, wiki, etc.). The footnotes show what CMMC and NIST 800-171 requirements are addressed.

Procedures are generally the most time-intensive component of cybersecurity documentation. The CSOP does the heavy lifting to get the template established, but your organization has to fill in the details that only your subject matter experts know.

SYSTEM SECURITY PLAN (SSP) TEMPLATE

This SSP template is based on the FedRAMP R5 template, but tailored for DFARS requirements and NIST 800-171 CUI controls.

Consider the SSP a "living document" that you keep coming back to and improving as you learn more about your environment or as processes evolve.

Expect the SSP to be one of the first things requested by a CMMC assessor, since it is the best method for the assessor to understand the who/what/where/why/how of your cybersecurity program.

COMPLIANCE REFERENCES

The NC3 not only contains crosswalk mapping for NIST 800-171 and CMMC to the NCP's policies, standards and procedures, it contains helpful charts, assessment criteria and other information to help comply with NIST 800-171 and CMMC requirements.

The crosswalk within the NC3 contains mappings for the CDPP and general CMMC-related mapping that is a valuable reference to understand the relationship with other compliance requirements.

SUPPLY-CHAIN RISK MANAGEMENT

This document focuses on External Service Provider (ESP) Management that is intended to help structure your approach to supply chain security and inform your service providers as to their cybersecurity obligations under NIST 800-171 and CMMC.

The ESPM is meant to be the playbook for how your organization managed supply chain-related risk and security concerns. The information from the ESPM can be used to help populate the Supply Chain Risk Management Plan (SCRM Plan).

SCRM PLAN

NIST 800-171 R3 3.171.1 has a requirement for a SCRM Plan and this document is designed to address that need.

This document is based on the SCRM Plan as specified in DI-MGMT-82256A. This format succinctly summarizes your overal SCRM-related activities.