STEP 1: PREPARE (System Level)

TABLE 2: PREPARE TASKS AND OUTCOMES—SYSTEM LEVEL

Tasks	Outcomes
TASK P-8 MISSION OR BUSINESS FOCUS	• Missions, business functions, and mission/business processes that the system is intended to support are identified. [*Cybersecurity Framework*: **Profile**; **Implementation Tiers**; **ID.BE**]
TASK P-9 SYSTEM STAKEHOLDERS	• The stakeholders having an interest in the system are identified. [*Cybersecurity Framework*: **ID.AM**; **ID.BE**]
TASK P-10 ASSET IDENTIFICATION	• Stakeholder assets are identified and prioritized. [*Cybersecurity Framework*: **ID.AM**]
TASK P-11 AUTHORIZATION BOUNDARY	• The authorization boundary (i.e., system) is determined.
TASK P-12 INFORMATION TYPES	• The types of information processed, stored, and transmitted by the system are identified. [*Cybersecurity Framework*: **ID.AM-5**]
TASK P-13 INFORMATION LIFE CYCLE	• All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system. [*Cybersecurity Framework*: **ID.AM-3**; **ID.AM-4**]
TASK P-14 RISK ASSESSMENT—SYSTEM	• A system-level risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]
TASK P-15 REQUIREMENTS DEFINITION	• Security and privacy requirements are defined and prioritized. [*Cybersecurity Framework*: **ID.GV; PR.IP**]
TASK P-16 ENTERPRISE ARCHITECTURE	• The placement of the system within the enterprise architecture is determined.
TASK P-17 REQUIREMENTS ALLOCATION	• Security and privacy requirements are allocated to the system and to the environment in which the system operates. [*Cybersecurity Framework*: **ID.GV**]
TASK P-18 SYSTEM REGISTRATION	• The system is registered for purposes of management, accountability, coordination, and oversight. [*Cybersecurity Framework*: **ID.GV**]

TASK P-8

TASK P-8 MISSION OR BUSINESS FOCUS	• Missions, business functions, and mission/business processes that the system is intended to support are identified. [*Cybersecurity Framework*: **Profile**; **Implementation Tiers**; **ID.BE**]

Information is elicited from stakeholders to acquire a more thorough understanding of the missions, business functions, and mission/business processes of the organization from a system security and privacy perspective.

TASK P-9

TASK P-9 SYSTEM STAKEHOLDERS	• The stakeholders having an interest in the system are identified. [*Cybersecurity Framework*: **ID.AM**; **ID.BE**]

Stakeholders include individuals, organizations, or representatives that have an interest in the system throughout the system life cycle—for design, development, implementation, delivery, operation, and sustainment of the system. It also includes all aspects of the supply chain.

TASK P-10

TASK P-10 ASSET IDENTIFICATION	• Stakeholder assets are identified and prioritized. [*Cybersecurity Framework*: **ID.AM**]

Examples of assets include:

- Computers
- Software
- Hardware
- Networks
- Data
- Business Processes
- Buildings

TASK P-11

TASK P-11 AUTHORIZATION BOUNDARY	• The authorization boundary (i.e., system) is determined.

Who gets access to what and how much access?

TASK P-11

A clear delineation of authorization boundaries is important for accountability and for security categorization, especially in situations where lower-impact systems are connected to higher-impact systems, or when external providers are responsible for the operation or maintenance of a system.

TASK P-12

TASK P-12 INFORMATION TYPES	• The types of information processed, stored, and transmitted by the system are identified. [*Cybersecurity Framework*: **ID.AM-5**]

What kinds of data are we dealing with?

TASK P-13

TASK P-13 INFORMATION LIFE CYCLE	• All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system. [*Cybersecurity Framework*: **ID.AM-3**; **ID.AM-4**]

Typical Information Life Cycle

- Information is created/collected
- Processed
- Usage
- Storage
- Disposal

TASK P-13

- How long are you required to store the different types of data?
- How is the data processed or used?
- What types of data are to be deleted and when?

TASK P-14

TASK P-14 RISK ASSESSMENT—SYSTEM	• A system-level risk assessment is completed or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]

Assessment of security risk includes identification of threat sources and threat events affecting assets, whether and how the assets are vulnerable to the threats,
the likelihood that an asset vulnerability will be exploited by a threat, and the impact (or consequence) of
loss of the assets

TASK P-14

Risk assessments are also conducted to determine the potential that the use of an external provider for the development, implementation, maintenance, management, operation, or disposition of a system, system element, or service could create a loss, and the potential impact of that loss

TASK P-15

TASK P-15 REQUIREMENTS DEFINITION	• Security and privacy requirements are defined and prioritized. [*Cybersecurity Framework*: **ID.GV; PR.IP**]

These requirements are based on the results of P-14

TASK P-16

TASK P-16 ENTERPRISE ARCHITECTURE	• The placement of the system within the enterprise architecture is determined.

Enterprise architecture is a management practice used to maximize the effectiveness of mission/business processes and information resources and to achieve mission and business success.

TASK P-16

Expected outputs include:

- Updated enterprise architecture
- Updated security architecture
- Updated privacy architecture
- Plans to use cloud-based systems and shared systems, services, or applications

TASK P-17

TASK P-17 REQUIREMENTS ALLOCATION	• Security and privacy requirements are allocated to the system and to the environment in which the system operates. [*Cybersecurity Framework*: **ID.GV**]

Requirements allocation identifies where controls will be implemented. The allocation of requirements conserves resources and helps to streamline the risk management process

TASK P-18

TASK P-18 SYSTEM REGISTRATION	• The system is registered for purposes of management, accountability, coordination, and oversight. [*Cybersecurity Framework*: **ID.GV**]

System registration, in accordance with organizational policy, serves to inform the governing organization of plans to develop the system or the existence of the system; the key characteristics of the system; and the expected security and privacy implications for the organization due to the operation and use of the system.