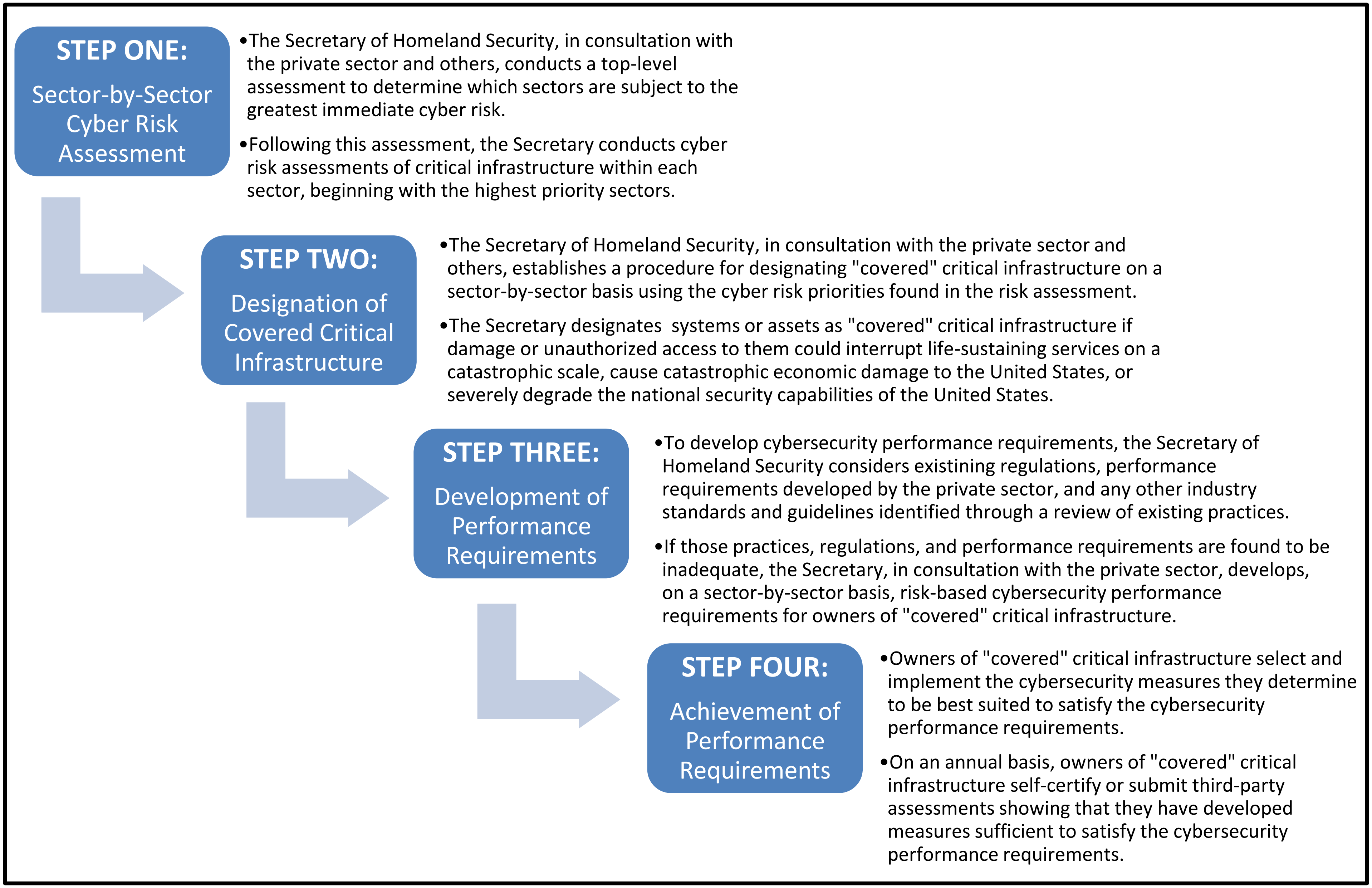
PROTECTING CRITICAL INFRASTRUCTURE IN THE CYBERSECURITY ACT OF 2012



STEP ONE: Sector-by-Sector Cyber Risk Assessment

- The Secretary of Homeland Security, in consultation with the private sector and others, conducts a top-level assessment to determine which sectors are subject to the greatest immediate cyber risk.
- Following this assessment, the Secretary conducts cyber risk assessments of critical infrastructure within each sector, beginning with the highest priority sectors.

STEP TWO: Designation of Covered Critical Infrastructure

- The Secretary of Homeland Security, in consultation with the private sector and others, establishes a procedure for designating "covered" critical infrastructure on a sector-by-sector basis using the cyber risk priorities found in the risk assessment.
- The Secretary designates systems or assets as "covered" critical infrastructure if damage or unauthorized access to them could interrupt life-sustaining services on a catastrophic scale, cause catastrophic economic damage to the United States, or severely degrade the national security capabilities of the United States.

STEP THREE: Development of Performance Requirements

- To develop cybersecurity performance requirements, the Secretary of Homeland Security considers existining regulations, performance requirements developed by the private sector, and any other industry standards and guidelines identified through a review of existing practices.
- If those practices, regulations, and performance requirements are found to be inadequate, the Secretary, in consultation with the private sector, develops, on a sector-by-sector basis, risk-based cybersecurity performance requirements for owners of "covered" critical infrastructure.

STEP FOUR: Achievement of Performance Requirements

- Owners of "covered" critical infrastructure select and implement the cybersecurity measures they determine to be best suited to satisfy the cybersecurity performance requirements.
- On an annual basis, owners of "covered" critical infrastructure self-certify or submit third-party assessments showing that they have developed measures sufficient to satisfy the cybersecurity performance requirements.