Table ES1. Metrics for Measuring the Performance of Critical–Infrastructure–Centric Cybersecurity Information Sharing

Inputs	Processes	Outputs	Outcomes
Shared information comprises both data and meaning: ▪ % of participating entities reporting that shared information received in a given time period contains both data and meaning ▪ % of submitted information and analytic products (based upon a random sample) that contain both data and meaning **Shared information is relevant:** ▪ % of participating entities reporting that the shared information they receive in a given time period informs decisions that reduce cyber risks to critical infrastructure ▪ % of participating entities reporting that the shared information they receive in a given time period contains new data, new meaning, or both ▪ % of *specific* information submissions or analytic products released in a given time period that inform decisions, and contain new data, new meaning, or both ▪ Number of instances in a given time period that *specific* submissions or products that were not yet known about led to the discovery of a previously unknown cyber incident, once deployed	**The goal is specified:** ▪ % of participating entities reporting that the goal has been developed, issued, and disseminated by a coordinating body **The goal is agreed upon:** ▪ % of participating entities providing express or implied concurrence with goal **Participating entities are appropriate:** ▪ % of participating entities who meet specified criteria ▪ % of participating entities who report that they can generate, analyze, or use information to achieve the goal **Entities are participating:** ▪ % of entities logging on to the information sharing website at least once in a given time period ▪ % of entities sending information to the website at least once in a given time period ▪ % of entities receiving information from the website at least once in a given time period ▪ % of entities participating in scheduled collaborative exchanges in a given time period ▪ % of entities with at least one person on the NCCIC floor at least once in a given time period ▪ % of entities who report independent collaboration with other entities in a given time period ▪ % of entities responding to RFIs in a given time period	**Information is used for tactical and strategic purposes:** ▪ % of participating entities reporting use of shared information to improve or implement security controls in a given time period (tactical use) ▪ % of participating entities reporting use of shared information to inform resource allocation decisions in a given time period (strategic use) ▪ % of received (i.e., accessed) information used to improve or implement security controls in a given time period (tactical use) ▪ % of received (i.e., accessed) information used to inform resource allocation decisions (strategic use)	**Goal is achieved** (all in a given time period): ▪ Number of incidents causing unavailability of critical services and estimated associated costs of damage ▪ Number of incidents causing the loss of critical data and estimated costs of damage ▪ Number of detected incidents, both prevented and successful, and estimated costs of damage ▪ Unplanned downtime ▪ Mean time to incident detection ▪ Mean time to incident remediation ▪ Mean time to incident recovery ▪ Mean time between failures