BIRD Cyber 2022
Explanation of Topics

Topic	Description
1. Secured Architecture for Protecting Core Operational Processes	The solution should demonstrate a holistic approach to protect key Operational Technology and Industrial Control System processes within a major operational critical infrastructure utilities (such as Water, Industry 4.0, Transportation, and Oil &Gas). There should be an emphasis on external connectivity with innovative online artificial intelligence optimization services in the cloud.
2. Small to Medium Airports or Seaports Real-Time Risk Assessment Solution Pilot	The solution will provide continuous cyber-posture visibility & situational awareness for EITHER small to medium airports OR small to medium seaports challenged to meet cybersecurity regulations released by sector-specific government agencies and industry associations. The solution should include a fusion of various sources such as external attack surface management, vulnerability assessment (IT & OT) & management, breach & attack simulation (BAS), passive network sensors, endpoint sensors, IoT analytics tools, and threat intelligence.
3. Piloting Resilience Centers for Small and Medium Businesses and Enterprises	Focusing on sectoral hubs*, the solution should demonstrate resilience centers capable of serving hundreds of entities, and including capabilities such as continuous monitoring, detection and response, online risk assessment services, cyber insurance, training & awareness, and other professional, financial and technological services, which are tailored to the challenge of working at scale, in a highly cost effective and distributed manner. **Sectoral Hubs are defined here as associations or other entities which typically engage/serve a substantial number of organizations from the same market sector.*
4. Advanced Data Fusion and Analytics	Developing and piloting data fusion architecture by collecting unstructured data from a diverse set of feeds (such as commercial threat intelligence, deception technologies, DNS data, malware samples, and inline sensors) and using AI/ML techniques to effectively identify Advanced Persistent Threats. Additionally, develop AI/ML infrastructure, algorithms, and tools to enable Security Orchestration, Automation, and Response, behavioral anomaly detection, data reduction, tipping and queuing of analyst workflows, and other useful mission needs. A particular use case of interest is the ability to generate representative training data that can be shared among partners including Government to Government and Government to Private Sector.