DoD Cyber Strategy
Needs Statement

The Department of Defense, Rapid Reaction Technology (RRTO) Innovation Outreach Program will conduct a Solutions Meeting in the Washington, DC area in June/July 2016. The Solutions Meeting provides selected innovative companies an opportunity to make short technical presentations to government representatives about their technologies and capabilities. There is the potential that companies may be selected for pilot projects or experimentation if their technology appears to match the needs described below.

The Department of Defense is looking for innovative technologies and capabilities in the following topic areas:

Cyber Situational Awareness
- Monitoring Missions, Threat Environments and Intrusion Responses
- Data Collection, Aggregation, Correlation and Dynamic Visualization
- Mapping Wired/Wireless Networks, Systems, Activities and Detecting Changes
- Behavior, Pattern, and Context Recognition
- Wireless Spectrum Monitoring
- Rapid Mapping of Business Functions to Cyber Assets

Wireless, Embedded and Industrial Control Systems (ICS)
- Network Discovery and Mapping for Wireless and ICS Networks
- Monitor and Recognize Control System Deviations
- Control Systems Situational Awareness
- Cyber-Physical and Internet of Things Security
- ICS and SCADA Centralized Security Management
- High Availability Systems Live Patching
- Malware Monitoring and Vetting Apps in App Stores
- Hardware-Based Security for Mobile Devices
- Position, Navigation, Timing Systems Synchronization
- Low Power Encryption

Next Generation Malware Detection, Adaptive Defense & Response
- Non-Signature-Based Detection
- Lightweight Behavior-Monitoring Agents (for Malware, Phishing, other Adversarial Behaviors)
- Discover and Isolate Malicious Activity in Background Noise
- Moving Target Defenses
- Malware Fingerprinting

Cyber Modeling & Simulation
- Cyber Attack Effects Simulations, Emulations and Automated Red Teams
- Scalable and Rapidly Reproducible Heterogeneous Environments
- Commercial Mobile and Control System Device Emulation
- Simulated Industrial Control Systems and Plants
- Realistic and Dynamic Traffic Generation (Wired and Wireless)
- Modeling Multi-Level Intrusion Incident Responses

- Multi-Agent Gaming Techniques
- User Behavior Models
- Cyber Risk and Impact Models

Insider Threat Detection & Mitigation
- Human/System Baselining, Profiling and Analysis
- Intelligent, Adaptive Anomaly Detection
- Credential Theft Analysis and Detection
- Data Loss Detection and Prevention
- Social Factors Integration

Cyber Forensics & Analytics
- Automated Electronic Evidence Discovery
- Information Discovery and Dynamic Sensing
- Real Time Classification and Correlation of Network Captures and Host-Level Events
- Multi-Source, Multi-Time Scale Data Analytics for Data Fusion
- Inspect and Trust Encrypted Traffic Crossing Network Boundaries

Enterprise & Cloud Security Services
- Multi-Level of Security for Application and Cloud Development
- Technologies for Deploying Sensors and Probes at Scale
- Automated Network Discovery and Configuration
- IP and Non-IP Address Mapping and Visualization
- IP-Enabled Command and Control Paths
- Resource Management Access and Authority Controls
- Enterprise Data at Rest/In Use/In Transit Encryption
- Seamless Integration of Security Hardware and Software
- Penetration Testing Tools
- Security Assured Software Development
- Vulnerability Assessment
- Application Scaling and Protection
- Real-Time Cloud Analytics

Big Data for Cyber
- Validated and Non-Validated Source Integration
- Analytics and Analytical Workflow Automation
- Batch, Interactive and Stream Processing
- Data Management and Stewardship

Artificial Intelligence/Autonomy for Cyber
- Autonomous Planning and Reasoning
- Cognitive Agents
- Swarming Agent Technologies
- Agent Scalability and Miniaturization
- AI for Cyber Analytics

Companies interested in participating in the Solutions Meeting should submit an application to RRTO Innovation via e-mail to osd.pentagon.ousd-atl.mbx.rrto-innovation@mail.mil.

The following information is required in the application (Note: Only 1 application is permitted per company):

1. Email subject line: "DoD Cyber Strategy Solutions Meeting Application"
2. Company name
3. Website address
4. POC, email, phone number and an alternate POC if desired
5. A succinct description (less than 100 words in length) of the company's technology that it proposes to present at the Solutions Meeting
6. Map the technology to the Needs Area you believe best fits your solution

All applications must be received on or before 5:00 PM EDT, April 19, 2016.

Selected companies are responsible for their travel and all other expenses associated with participation in the DoD Cyber Strategy Solutions Meeting.