C2/C4I/CYBER	
BLUF TITLE	**BLUF STATEMENT**
Secure IoT Manufacturing System	The use of the Internet of Things (IoT) is gaining interest in manufacturing systems because it allows such systems to improve their efficiency. Unfortunately, the use of IoT creates cybersecurity vulnerabilities, which could ultimately sabotage and introduce defects into the manufacturing system. One group of possible sabotage attacks is the defect injection (DI) attack. This attack causes objects to be fabricated with deformed geometry, weak material composition, and other flawed characteristics. The presented technology is a method to detect compromised machines in IoT-enabled manufacturing systems. The method uses energy consumption and voltage measurements to identify compromised machines.

Altor-GRC, Inc. - Data Enclave™ Formulary	AltorGRC's Data Enclave™ Formulary solution(s) fully integrated Cyber Risiliency. The Why: A few years back we heard a story that defined consequences of data latency within military communications. Troops on the ground radioed for air support and gave their coordinates. By the time support arrived, the troop action on the ground had moved to new coordinates, they had sent a communications update with new coordinates. Due to latency of the data in the communications systems, there were friendly losses due to troop movement during the live situation. Disparate data is hard to move between systems and slows processing. It presents data integrity issues and system of record consequences. It's costly, time consuming, and difficult to apply analytics to that will yield assistance with decisions, assessments, gap analysis, security. Think of our technology, as providing data efficiencies that affect, communications, security, cost, time, gap identification and added security thru simplification yielding expanded analytics. Fully integrated Cyber Resiliency for a business or government agency no matter the data or system type = agnostic technology. Think of this as a type of back end digital transformation. Bain published in September of 2021 to the WEF what they have named Traceability Transformation Platform builds for those clients that would like to shed the entire technology ownership.

Multi Cloud Data Loss Prevention	In the rising paradigm of cloud computing, attainment of sustainable levels of cloud users' trust in using cloud services is directly dependent on effective mitigation of its associated impending risks and resultant security threats. Among the various indispensable security services required to ensure effective cloud functionality leading to enhancement of users' confidence in using cloud offerings, those related to the preservation of data privacy are significantly important and must be matured enough to withstand the imminent security threats. We intent to leverage the metadata stored in cloud's data repositories in order to defend the privacy of users' data items stored using a cloud provider's metadata service. Using the sensitivity parameterization parent class membership of cloud data attributes, the database schema is modified using cryptographic as well as relational privacy preservation operations.
Private Cloud Technologies include Edge Compute Solutions	Awnix provides an "Emporium of Compute Products and Services" including but not limited to centralized private cloud base on OpenStack and/or K8s. Awnix also is offering edge compute products and services that are designed to enable emerging markets like 5G and grow existing markets like IoT. Simply put Awnix works with a range of Telco and Gov clients to produce comprehensive cloud solutions with heavy focus on security and innovation.
BaseConnect Enterprise Communication, Emergency Management and Recall Application	BaseConnect is an enterprise mobile and web application that saves lives, time, and resources by using social-media technologies in a secure and structured environment. We also streamline critical communication processes to effectively communicate during emergencies allowing for real-time analytics of which member has or has not received critical information during emergency accountability recalls.
Quantum-resistant, end-to-end encrypted email service	Blinkly is a quantum-resistant (i.e., secure against an attack by a quantum computer), end-to-end encrypted (i.e., prevents third-parties from accessing data) email service that provides the highest level of encryption. Blinkly improves upon the AES-256 encryption, which is endorsed by the NIST as a quantum-resistant protocol, by increasing the algebraic complexity to improve security. Blinkly is a stand-alone platform that can communicate with all other email services. It is accessible via a web browser and can be deployed in the cloud or on-premise.
Borsetta's patent pending technology connects physical assets to our AI Asset Management Platform to secure real-time information and process intelligent actions via a trustworthy edge network	Today the collection, processing, and dissemination of data across all domains is overly burdensome and slow. In order to win tomorrow every asset must be trusted to connect, share, filter and learn in real time. So, how do we bridge the gaps between disparate assets and networks across all domains. Borsetta's mission is to secure a hyperconnected world with trust, where every asset, device or object has the capability to self authenticate, transact, sense its environment, transmit secure real-time information and process intelligent actions via a trustworthy edge network.

Communication system for a definable/decentralized community with multiple levels of access based on assigned authorities/permissions.	OneRoom is a cloud-based communication/user engagement platform transforming how different groups of people (stakeholders), the organizations to which they belong and its partners, connect and communicate. OneRoom recognizes the unique role, tasks, goals and communication needs of each audience. OneRoom streamlines communication by replacing paper documentation, phone/robo calls, text messages and the need for using multiple applications, with an easy-to-use, intuititve interface that pioriritizes communicaiton, allows quick and easy task execution. OneRoom empowers users by giving them control; allowing them to manage tasks and information better, faster and easier to help them be more organized and successful.
We Separate IT From OT and Make OT INVISIBLE on the Internet!	Secure-IoT provides a physical and cyber security solution to end the threat of vulnerable endpoint operational devices. With SC-IoT technology, organizations can employ consistent security solutions with centralized management across the extended network. Secure-IoT is a managed service platform that protects the Operational Technology (OT) of enterprises by providing secure, private networks and managed communications, ensuring safe operations without compromise. Control Systems and devices (i.e., things) that run inside our Virtual Enclaves become invisible to hackers & accessible only to authorized users.
Time, Expense, Referral, Data Sharing	Our software enables secure data collaboration among teams or coalitions.
Arytic: NextGen AI Predictive Hiring PlatformH Platform	Arytic is an Artificial Intelligence Hiring Platform. It is an intelligent match machine removes unconscious bias and measures psychometrics or personalities, assesses skills, job, and team fit to align with the company's culture. It can be tailored for the culture and employment rules of a specific organization, such as the Department of Defense. It will revolutionize the hiring process, ensuring that newly hired DoD civilian talent is highly compatible to support the global warfighting mission of the DoD. Arytic has demonstrated a significant return-on-investment from creating the first-time fit, thereby enhancing retention, and limiting personnel turnover.
The Athena Project	The Athena Project grew from experiences in the military where reports written did not translate to reports read, let alone lessons learned. The Athena Project has a unique ability to: Collect and signify narrative stories of a human (complex) system at scale; Reduce the cognitive bias in human system mapping through AI tools; Identify the emerging trends and risks associated with a given human system. The tools used to accomplish this enable key decision makers within organizations to understand complex environments. The Athena Project's dynamic capacity and capability provide the space and insights for better decisions about critical strategic and operational outcomes.

Intelligent Integrator-Secure	The IT Consulting industry and custom data integration efforts have compelled organizations to forego innovation to attempt to tame the plethora of existing data and sort the new data being created every day. What if there is an easy-to-use solution that unifies data integration and knowledge-based decision making at the operational leader level? The Intelligent Integrator platform is a paradigm shift in enterprise level knowledge-based decision-making for organizations of all sizes.
Roadfi – Self-contained Portable Off Grid High Speed WiFi System	ISEEYOU360 Roadfi is a self-contained portable high-speed connectivity Wi-Fi system contained in a ruggedized case for use in austere locations. Roadfi includes a mobile router, antenna array, powered by ac/dc solar or mobile power pack which stays running for 1-5 days depending on model and battery options. Roadfi provides high speed internet and voice communications to any Wi-Fi enabled device. Supports multiple simultaneous users, can be used in almost any location and highly sensitive antennas can receive cellular signal from extreme distances. Protects sensitive data using the most secure platform found in any mobile connectivity device.
REAPR - Precise Electronic Warfare – Terrestrial and Group 3 UAS (Textron Shadow)	The REAPR (Reactive Electronic Attack Portable Radio) is a full featured Electronic Warfare (EW) solution available as a ground-based model or on a Group 3 UAS, the Textron Shadow. This precise EW solution can automatically identify and classify adversaries' target signals, geolocate them and, optionally, jam/disrupt them without disrupting Blue Force signals. REAPR nodes operate in networked or stand-alone mode. Intuitive HQApp enables end users to operate the REAPR system locally or remotely and change mission parameters on-the-fly when necessary. Supports 70 MHz to 6.0 GHz. Open architecture supports RaptorX and can be integrated into other TDOA networks.
Plasticity Disinformation Toolkit	Plasticity's Disinformation Toolkit helps intelligence analysts find the "needle" in the "haystack" of publicly available information like social media, news, and the dark web. The toolkit improves content searching and automatically flags content that may be disinformation, bot activity, or a coordinated narrative by a state/non-state actor. Intelligence analysts can then analyze or translate content and easily generate aggregate reports to pass up the chain of command. Plasticity's tool helps analysts — who have remained relatively constant in numbers over the years — keep up with the exponentially growing quantity of online content.

PA File Sight: Cyber Defense: Protecting Critical Data	Detects and blocks users copying files from Windows file servers Detects and blocks ransomware encrypting files on servers Blocks client USB drives with option client agent Reacts in real-time, with automatic actions and alerts Records IP address, user account, computer name Threats automatically and immediately shared among protected servers so they can protect themselves Reports to see who accessed what, when, and from where
Skymerx Technologies	Skymerx Technologies, a traffic data consultative group has developed a leading edge algo-driven transformative software platform that analyzes traffic video content and provides automated reports (volume, speed and, classification) back to customers.
Passwordless Bio-metric Multi-factor Authentication to meet new cyber security standards	SOFTwarfare® is an American cyber security software manufacturer. Our flagship patented product, BioThenticate®, is a trusted passwordless multifactor authentication solution that enables corporations and government agencies to meet new industry and government standards for authentication. BioThenticate supports multi-modal biometric authentication services such as fingerprint, facial recognition, iris, voice, hand geometry, retina and traditional push notifications. Fully integrated into existing technical infrastructure that is on-prem, or in multi-cloud hybrid environments, BioThenticate gives customers the ability to secure their user base rapidly taking their environment passwordless. BioThenticate is fully integrated into existing technical infrastructure through use of secure hardened API integration on the proprietary and patented solution, PangaeAPI®, by SOFTwarfare. We truly partner with our customers to realize the mission to secure infrastructure modernizing authentication and integration methods allowing you to *defend your assets against cyber attack*®.

Accessible Industrial IoT Technology – Easy to Adopt, Straightforward to Use	Our software helps organizations use off-the-shelf IoT sensors (RFID, barcodes, GPS, and more), digital forms, and algorithms and data models to: * Automate manual processes * Eliminate paper and spreadsheets, and make data accessible where it is needed, when it is needed, at all levels of the organization * Improve operational visibility, including ensuring activities are performed on time, every time and exceptions are flagged in real-time * Optimize operations and eliminate surprises regarding the location, condition, and stocks of assets Gain the benefits of advanced technologies without needing large company resources.
Real-Time Autonomous Protection for Detecting and Remediating Cyberattacks	Synaptic has developed a revolutionary autonomous Native Linux Platform (NLP), purpose-built for detecting and remediating Linux cyberattacks in real-time. Current COTS EDR products are passive and focus only on prevention, failing to detect sophisticated Linux attacks effectively, and can take up to six minutes to provide an alert. Synaptic's patent-pending, autonomous AI/ML-based platform provides extremely low-security overhead using <5% of the CPU; is >99% effective at detecting and stopping attacks against Linux systems; operates at machine speed to detect an attack in milliseconds with false-positive rates of <5%; and works in connected, disconnected, and air-gapped environments.
Platform Interoperability Across Your Information Supply Chain	BFC's aDAPt solution is a highly scalable IT resource orchestration product that centralizes the management and control of disparate technology assets into vendor-agnostic and intuitive user-experience. With aDAPt, organizations create a global command and control strategy for assets that move data from the point of creation, through its use, and to its disposition. aDAPt empowers users by giving them informed insights and the controls to ensure full technology utilization.

IoT Enablement Company – Track, Monitor, Control - Anything/Anywhere Securely	As an end-to-end solutions provider in the IoT space, Viaanix manages all aspects of the customer’s solution: conceptualizing hardware, designing software, integrating the two, and manufacturing components. We specialize in IoT, emphasizing industrial internet that focuses on M2M communication. We create smart systems for manufacturing industries, logistics, defense, transportation, government, healthcare, homes, and cities. Viaanix proudly states that we are the only company in the world which designs, manufactures, and distributes its hardware and software. Through this process, Viaanix has the flexibility of quick changes, customization, and adjustments to hardware or software as needed—without incurring high costs
SMARTTM Sensor Network	A rapidly deployable low power wireless mesh network unattended ground sensor intrusion detection system that uses communication link quality between nodes to detect intrusions. The nodes can be placed or tossed in the desired area without the need for extensive planning. It includes a graphical user interface using maps to remotely identify location of deployed nodes and image recognition capability to identify contacts of interest or intruders.