

# Cyber Lab-as-a-Service (IPKeys CLaaS<sup>®</sup>)

**A unified, AI-fueled business intelligence reporting and analytics platform optimized and ready for use by the Department of Defense (DoD).**



This submission includes data that shall not be disclosed outside the Government, except to non-Government personnel for evaluation purposes, and shall not be duplicated, used, or disclosed -- in whole or in part -- for any purpose other than to evaluate this submission. If, however, an agreement is awarded to this Company because of -- or in connection with -- the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent agreed upon by both parties in the resulting agreement. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in all pages of this document.



## Today's Challenge

[Hackers attack every 39 seconds on average](#), which makes maintaining the cybersecurity of Department of Defense Information Technology platforms within the DODIN an increasingly difficult task. Protecting our most critical national security network while meeting or exceeding compliance requirements can overrun personnel and budget constraints very quickly. How do we ensure attackers don't have the advantage relative to our ability to avoid threats and remain compliant?

## The Solution

Accurate and timely information is key to staying ahead of cybersecurity threats and maintaining compliance. The vision of a "single pane of glass" that provides fast, accurate information is made real through IPKeys' **Cyber-Lab-as-a-Service**. It provides automated, real-time visualizations of disparate risk management framework (RMF) cybersecurity data and processes. It correlates this information with GRC requirements, making it easier to maintain both cybersecurity and compliance.

## What is IPKeys CLaaS®?

IPKeys CLaaS® is a unified, AI-fueled business intelligence reporting and analytics platform. It allows for the continuous monitoring of all cybersecurity information contained in your environment. Through IPKeys CLaaS® your information is presented in a way that is consumable and actionable - and mapped to critical compliance requirements.

It contains an intuitive toolset that empowers users to make better cybersecurity decisions, while placing the power of interactive analytics at their fingertips. This allows for the creation of customized data stories and visual reports that aid in fast accurate decision making.

Built on existing commercial technology, it contains a proprietary correlation engine that brings cyber monitoring, alerting and compliance together into one tool.

### Key Features:

- Nine standardized dashboards that provide both wide and deep coverage of the most critical cybersecurity information
- A unique many-to-many associative data analytic capability, which is critical for analyzing, describing, and training on vulnerabilities/security issues across cybersecurity standards
- Customizable alert thresholds and objectives that eliminate the need for continuous monitoring by a human.
- Integration with Office 365 and Microsoft Active Directory
- Flexible deployment options: on and off premise configurations including a standalone server, virtualized appliance or FedRamp Cloud



## Designed for Today's Cybersecurity Environments

IPKeys CLaaS® was built from the ground up to address the needs of both cybersecurity and compliance professionals in a wide range of industries. It is the result of IPKeys unique expertise in high-risk cybersecurity and compliance.

**High Performance** Provides a quick and efficient way to visualize RMF scan data in real-time. It works in computer memory to meet performance expectations for an enterprise environment.

**Flexible** Infinitely configurable, allowing users to view information how they want to in lieu of pouring over numerous data sources, tools, spreadsheets, PowerPoints and documents.

**Detailed** Delivers a way to discover (or uncover) hidden data connections (e.g. Ransomware and Microsoft patches). Users can drill down into ever deeper levels of detail across the enterprise.

**User Friendly** Powerful, modern and simple web-based UI delivers a great user experience, with information clearly organized in dashboards. It makes it possible for any user to find and analyze cybersecurity data on their own, simplifying the cybersecurity process.

### Your Journey to a Mature Cybersecurity Process

IPKeys CLaaS® provides a unique burndown view of the ongoing vulnerability mitigation process. When viewed over time, this can present you a clear picture of new vulnerabilities and those being addressed, all by impact value - giving you a compelling picture



## What are the Benefits of Using IPKeys CLaaS®?

The primary goal of IPKeys CLaaS® is to help cybersecurity professionals make better decisions. By collecting, organizing and presenting the overwhelming amount of cybersecurity information in a clear, actionable way -- then connecting it with the compliance requirements, we've built the next generation of cybersecurity tools for the DoD. IPKeys CLaaS® increases the velocity at which you can address cybersecurity and compliance issues, reducing cost and compressing timelines.

How do I:	How IPKeys CLaaS® Helps:
Identify and measure risk?	By calculating, identifying, quantifying, and visualizing risk using authoritative and correlated cybersecurity data
Minimize or eliminate documentation?	By generating dynamic reports using data story templates populated with latest cybersecurity data
Optimize processes that are typically very slow?	By automatically generating the Plan of Actions and Milestones (POA&Ms) and calculating the Rough Order of Magnitude to mitigate vulnerabilities
Produce scans and assessments that provide material findings aligned with the FedRamp and CNSSI 1253?	By immediately visualizing Cloud Service Providers (CSPs) Impact Levels and by dynamically changing CSPs and Information Systems security baseline
Avoid manual entry of voluminous amounts of data?	By using authoritative cybersecurity sources it removing manual / human entry - eliminating human error
Determine what information provides value to assessing risk?	Clear text search and on-the-fly calculation, statistics, filtering and aggregation instantly updates all analytics with each click
Deliver monthly and regular reporting?	Rapidly visualize and report each CSP offering or Information Systems for compliance and generate a "one pager" dynamically / monthly

## How is IPKeys CLaaS® Optimized for the DoD?

The DOD relies on a variety of military and civilian personnel to conduct cybersecurity support through IAW NIST SP 800 series and RMF processes for Authorization to Operate (ATO) and continually monitoring assets on the DODIN. These Risk Management requirements are burdensome, time-consuming and costly without enterprise cybersecurity capabilities and automation such as IPKeys CLaaS® for continuous ATO.

Developed in concert with DISA and built on IPKeys' deep experience with the DoD, IPKeys CLaaS® is singularly optimized to meet the mission need of cybersecurity and compliance professionals in the DoD. In particular, we focused our development on the needs of Program Executive Officers and Authorization Officers require that interactive business intelligence to make critical risk decisions to support cyberspace operations of Information Systems and Cloud Service Provider (CSP) Offerings (CSO).

### The Genesis of IPKeys CLaaS® with DISA

IPKeys' provided cybersecurity services to 26 enterprise cyber programs. We developed and set in operation the Mission Assurance Consolidated Development Laboratory (MACDL) within the DISA facility which served as a communication hub between JITC, multiple DISA PMs, capability developer vendor teams, end users, and the services. IPKeys developed and implemented a Baseline Control Process (BCP) to facilitate cooperation between stakeholders and coordinate the sharing of information, risk assessment, test strategies, test tools, reports, and resources. We supported system



baseline control, CM, firewall implementation, intrusion detection systems (IDSs), continuous monitoring, security, and developmental test & evaluation (T&E) using a centralized consolidated test bed environment. IPKeys fulfilled IAVA compliance with 60,000+ security patches and hot fixes. We consolidated Risk Management Framework (RMF) artifacts and leveraged automated validation capabilities.

## Standard Dashboards

IPKeys CLaaS® comes with out-of-the-box functionality that is game changing for organizations and their cybersecurity programs. These standard dashboard give you a broad, real-time view of cybersecurity and compliance.

<b>AO/ Senior Management Dashboard</b>	Consolidated cybersecurity data for all programs/offerings allowed by the authorization boundary of the management role.
<b>Authorization Overview</b>	High level of details, dates, values, and scans over time.
<b>Continuous Monitoring Report</b>	Unique and raw scanning data summaries, with open items within monthly intervals. Flexible time period options.
<b>Mapping</b>	Asset and inventory level details of the security boundary.
<b>Sensing</b>	Rough Order of Magnitude (ROM) to mitigate findings. Group vulnerabilities by NIST security control families. Autogenerate Plan of Action and Milestones (POA&M).
<b>Responding</b>	Burndown view to illustrate cybersecurity process maturity over time. Includes breakout of vulnerabilities grouped by CAT I, II and III.
<b>Static Code Analysis</b>	Display Fortify data for software development systems.
<b>CAT I Priority List</b>	Provide the burndown of CAT I vulnerabilities list and diagram as well as forecast values for a 24-month period.
<b>CAT II Priority List</b>	Provide the burndown of CAT II vulnerabilities list and diagram as well as forecast values for a 24-month period.
<b>CAT III Priority List</b>	Provide the burndown of CAT III vulnerabilities list and diagram as well as forecast values for a 24-month period.

## Want to Learn More?

We're passionate about supporting the DoD's mission through superior technology and services. Reach out to us to answer your questions, request a demo or visit one of the contract vehicles to learn more about how IPKeys CLaaS® can help you.

Program Contact:

**Art Clomera**

Chief Technology Officer  
aclomera@ipkeys.com  
(540) 628-7555



Contract Holder

[Request a Demo](#)



## About Us

IPKeys delivers innovative cyber security and technology solutions focused on reducing risk and driving efficiency to help protect North America's most critical organizations, industries and resources.

## IPKeys Technologies

IPKeys Technologies is focused on protecting the US government's critical data, systems & people with the most advanced and secure technology solutions.

**IPKeys Technologies**

www.ipkeys.com  
10 Center Street  
Suite 201  
Stafford, VA 22556  
(540) 657-4717