IPKeys Product Brochure

Cyber Lab-as-a-Service (IPKeys CLaaS®)

A unified, AI-fueled Risk Management Framework (RMF) automation reporting and analytics platform optimized and ready for use by US federal government agencies.



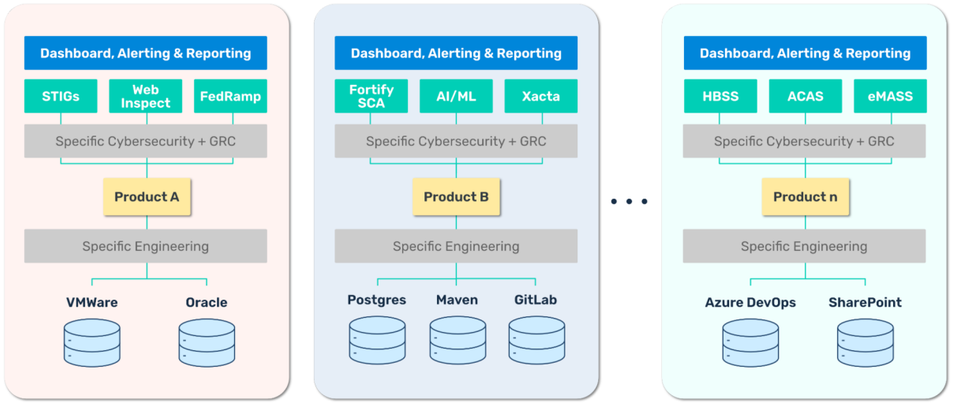
This submission includes data that shall not be disclosed outside the Government, except to non-Government personnel for evaluation purposes, and shall not be duplicated, used, or disclosed -- in whole or in part -- for any purpose other than to evaluate this submission. If, however, an agreement is 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 networks while meeting or exceeding the compliance requirements of the Federal Information Security Modernization Act (FISMA) can quickly overwhelm personnel and budget constraints. How do we ensure attackers do not have the advantage relative to our ability to prevent attacks and remain compliant?

In today's RMF, product/programs and ATOs are silos managed by individual program managers. Ultimately, this results in zero efficiency in scale, with an overlap of common tools, personnel, and processes. Other major issues include:

- Identity and user management challenges as a result of individual tools
- Separated documentation, presentation, and reporting with limited or no sharing
- Human errors across a portfolio with inconsistent outputs



The Problem: Programs/ATOs are Silos

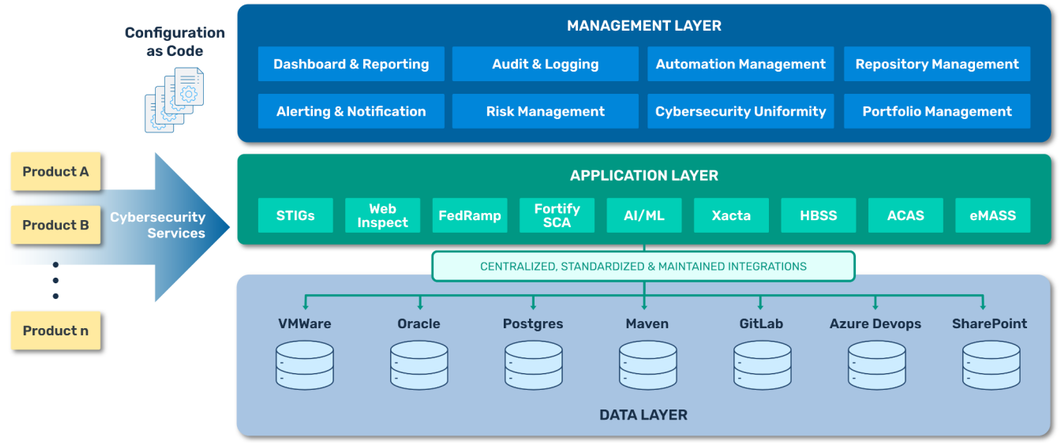
"Today, under RMF, we are still way too much paper-driven. We have to get to the point where we are data-driven." [1]

Roger Greenwell
Director of the Enterprise Integration and Innovation Center and DISA CIO



The Solution: A Unified Approach is Required

Accurate and timely information is key to staying ahead of cybersecurity threats and maintaining compliance. The ideal would be a centralized data repository for all products and authoritative data, plus an application layer for common interfacing with cyber systems (e.g. eMASS), scan tools (e.g. Fortify, HBSS, ACAS), and best practices (e.g. STIGs).



The Solution: A Unified Approach

This unified approach would include a management layer across all products, especially:

- Leader dashboard for risk management with built-in presenting and reporting capabilities
- Proactive alerting capability to notify cyber personnel when something needs attention
- Scorecard capability to track progress over time
- Automation for documentation generation and approval process (write once, then reuse for the enterprise)



"Wouldn't it be cool if...RMF was Operational and Continuous" [2]

Lt. General Robert Skinner
Director of Defense Information Systems Agency

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this submission.

Sources:
1: Greenwell, Mr. [Live stream]. YouTube. https://youtube.com/live/zKfGgDmff5k 39.23 / 51:17, pg 2
2: Skinner, LTG [Video]. YouTube. https://youtu.be/uEVV631kp2c, pg. 3
TechNet Cyber 22 [YouTube playlist]. YouTube. https://youtube.com/playlist?list=PLmnpZD8L9IYTSYxEoHUs1UjdUGjThSLKd

What is IPKeys CLaaS®?

This vision of a “single pane of glass” that provides fast, accurate information is made real through **IPKeys CLaaS®**. It provides automated, timely visualizations of disparate RMF cybersecurity artifacts and processes. It correlates the customer’s implementation against FISMA requirements, making it easier to maintain both cybersecurity and compliance.

IPKeys CLaaS® 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 tool set 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 proven 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 analytics 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 Microsoft SharePoint, Office 365 and 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 quickly. It works in computer memory to meet performance expectations for an enterprise environment.
Flexible	Dynamic and adaptable to the customer’s implementation, 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

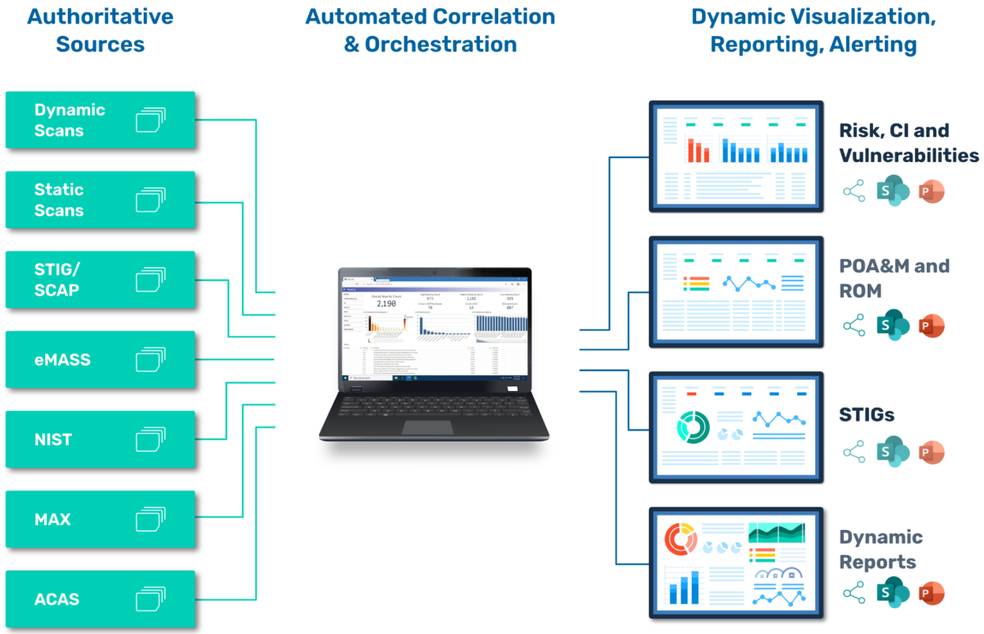
IPKeys CLaaS® provides a unique burndown view of the ongoing vulnerability mitigation process. When viewed over time, this can present you a clear picture of new vulnerabilities and those being addressed, all by impact value - giving you a compelling picture



Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this submission.

IPKeys CLaaS® Operational View

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 federal government. IPKeys CLaaS® increases the velocity at which you can address cybersecurity and compliance issues, reducing cost and compressing timelines.



IPKeys CLaaS® injects authoritative data to eliminate the "human-in-the-middle" processes. This includes data from/to enterprise capabilities (e.g., eMASS), hardening data (e.g., DISA STIGs), scan tools, standards (e.g., NIST 800-53 security controls, FedRAMP profiles, databases, and system interfaces. Data is curated and orchestrated IAW Standards and prepared for storage and use. IPKeys CLaaS® then provides dynamic visualization, reporting, and alerting capabilities to manage risk, drive programmatic (cost, schedule, and performance), ensure hardening of systems to acceptable risk tolerance, dynamically report progress and priorities of work, and plan for the future. All reporting and data outputs are available in standard formats, including Excel, CSV, HTML, XML, PowerPoint, Word, and PDF to ensure seamless integration with existing agency workflows and systems.

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 the US Government. 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 the 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 ingesting authoritative cybersecurity sources, it removes 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

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this submission.

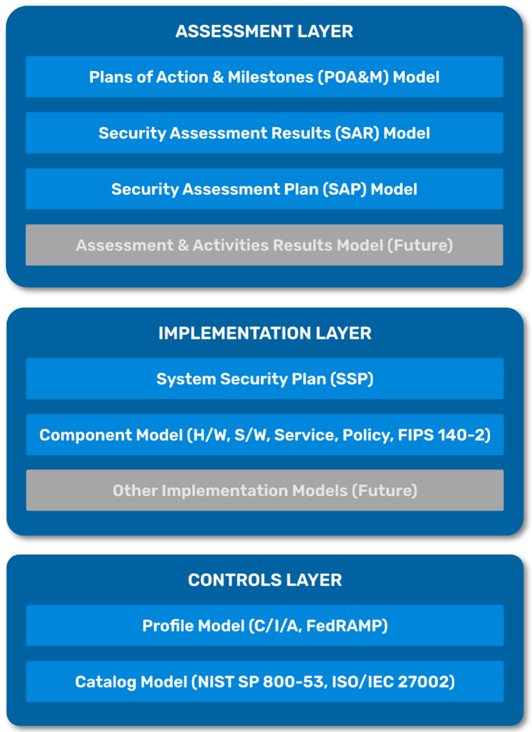
Leveraging OSCAL to Accelerate ATO

OSCAL represents a huge step forward towards automating and accelerating the painfully slow RMF process, but it remains unclear how best to leverage OSCAL to benefit agency programs. IPKeys' CLaaS is positioned to leverage emerging OSCAL capabilities to further accelerate your agency's ROI. As key agency systems (e.g. eMass, CAMS) develop and integrate OSCAL capabilities, IPKeys' CLaaS will be ready to leverage OSCAL to further automate and reduce the manual burden of getting to ATO. The emerging integration of OSCAL with IPKeys CLaaS will enable agencies to:

- Establish, receive, and share machine-readable control baselines for reciprocity
- Maintain, receive, and share actionable, up-to-date information about how controls are implemented in your systems
- Automate the continuous monitoring and assessment of your system control implementation effectiveness

CLaaS completion of the OSCAL architecture

NIST OSCAL architecture is organized in three layers with each layer in the stack providing information structures that are referenced and used by each higher layer. Each layer is composed of one or more models, which represent an information structure supporting a specific operational purpose.
IPKeys CLaaS provides the customer specific data to instantiate the Implementation (hardware, software, services, policy, process or procedure) and Assessment layers (planned, performed and how the results of assessment activities are reported)



Standard Dashboards

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

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

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this submission.

About IPKeys Technologies

IPKeys is a member of the Chickasaw Nations Industries family, with a focus on cybersecurity technology and expertise.

We revolutionize how federal agencies respond to evolving cybersecurity threats. Our expertise – paired with our innovative technologies – provide a game-changing approach to identifying and protecting critical assets.

What truly sets us apart, however, is our deep passion and commitment to help you achieve your federal government mission. We encourage you to contact our existing and former clients to validate this first hand.

Key Capabilities

Cybersecurity and Analytics

Protecting your critical data, systems & people with the most advanced and secure technology solutions.

Cloud & Data Center Engineering

Accelerating federal agencies journey to the cloud, securely.

Software & Systems Engineering

Developing security centric software and systems solutions to address high-impact, demanding missions.

Contract Vehicles

GSA MAS
GS-35F-419CA

RS3
W15P7T-19-D-0064

ITES-3S
W52P1J-18-D-A029

CIO-SP3 SB
75N98120D00128

SeaPort-NexGen
N00178-19-D-7886

Key Performance Examples

Cybersecurity and Analytics

DISA NETOPs/MACDL
Designed, implemented, and operated DISA's Mission Assurance Capabilities Development Lab (MACDL), providing a virtualized test lab integration and evaluation of enterprise cyber capabilities.

DISATASS
Provided agency-wide cybersecurity compliance services to the DISA Risk Management Executive that spans all seven RMF steps. These services include authorization and assessment for cloud and system implementation, review and continued authorization of systems, compliance monitoring, and conducting DoD risk management boards to assess the risk posed to the DoD GIG.

Cloud & Data Center Engineering

DLA
Implemented an ITIL-driven approach to support DLA's Federal Data Center Optimization Initiative (DCIO) initiative, consolidating data centers and migrating the cloud-ready application to MilCloud and Azure Clouds. Co-authored the DLA Cloud strategy and supported the architecture and instantiation of DLA's first accredited IL 4 and IL5 Azure cloud enclaves.

Software & Systems Engineering

DLA RPA
Developed, deployed and maintained hundreds of RPA bots for the Defense Logistics Agency reducing the burden on employees and contributing more than 130,000 hours to the DLA mission.

DRRS-A / ITEMSS
Delivered systems engineering expertise by providing requirements shells, use cases, SyRS, and external interface specifications for the GCCS-A readiness components (e.g.DRRS-MC, AdHoc Query and EIM.)

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this submission.

Want to Learn More?

We're passionate about supporting the federal government'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 Contacts:

R. Shawn Elliott
President and LLC Manager
shawn.elliott@chickasaw.com
(540)-226-3559

Brad Smith
Senior Program Manager
Brad.Smith@chickasaw.com

GSA Contract Holder

Request a Demo

IPKEYS

Chickasaw FEDERAL

