Justice IT Service Offerings

Cybersecurity Services

Reliable, competitively priced, and customizable services.

U.S. Department of Justice

Published September 2020

DOJ makes cybersecurity easy.

The U.S. Department of Justice's (DOJ's) holistic cybersecurity services are unmatched across the federal government, integrating comprehensive advanced threat intelligence that spans multiple federal agencies to proactively defend an organization from today's sophisticated cyber threats.

Bolster cybersecurity by detecting and stopping cyber threats, while improving Federal Information Security Management Act (FISMA) scores.

Contents

Introduction

The U.S. Department of Justice (DOJ) customizes cybersecurity services for any mission. Services are flexible and scalable to an organization's requirements. Accelerated acquisition and fast deployment fulfills cybersecurity needs quickly and efficiently.

Pricing is competitive and allows organizations to buy only the services they need, and a simplified interagency agreement process streamlines onboarding, enabling a quick transition to DOJ services.

Justice IT Services Offerings | Cybersecurity Services is a multilayered system designed to provide complete coverage to protect organizations from cyber threats.

Note

Access to DOJ information technology services is for federal agencies and organizations only. Services subject to change.

Innovative IT solutions.

Overview

Justice IT Service Offerings provide a full range of comprehensive cybersecurity services that shield enterprises against threats, while strengthening their cyber defense. This holistic approach enables enterprises to focus on their mission.

DOJ is designated by the United States Office of Management and Budget (OMB) as a federal shared service provider for Security Operations Center (SOC) services, supporting government-wide initiatives to consolidate and share services whenever possible.

DOJ cybersecurity services feature industry-leading technology with cybersecurity professionals, providing an unmatched capability to integrate advanced threat intelligence from across the federal government. And, all services are backed with responsive, reliable customer service.

Services

Cybersecurity Operations Services

Security Operations Center (SOC) Services

Insider Threat Prevention and Detection (ITPD) Services

Vulnerability Management

Penetration Testing

Cyber Threat Hunt Assessment

Anti-Phishing Program Support

Justice Cloud-Optimized Trusted Internet Connection Service (JCOTS)

Governance, Risk, and Compliance Services

Cybersecurity Policy Support

Information System Security Officer (ISSO) Services

Independent Security Control Assessments

Supply Chain Risk Management (SCRM)

Cybersecurity Assessment and Management (CSAM)

Cybersecurity Technical Services

Cost drivers

As an OMB-designated shared service provider, DOJ pricing achieves transparent cost recovery. Costs to deliver services vary based on the types of services required, as well as the size of the customer's enterprise, network and system complexity, and unique policies and procedures.

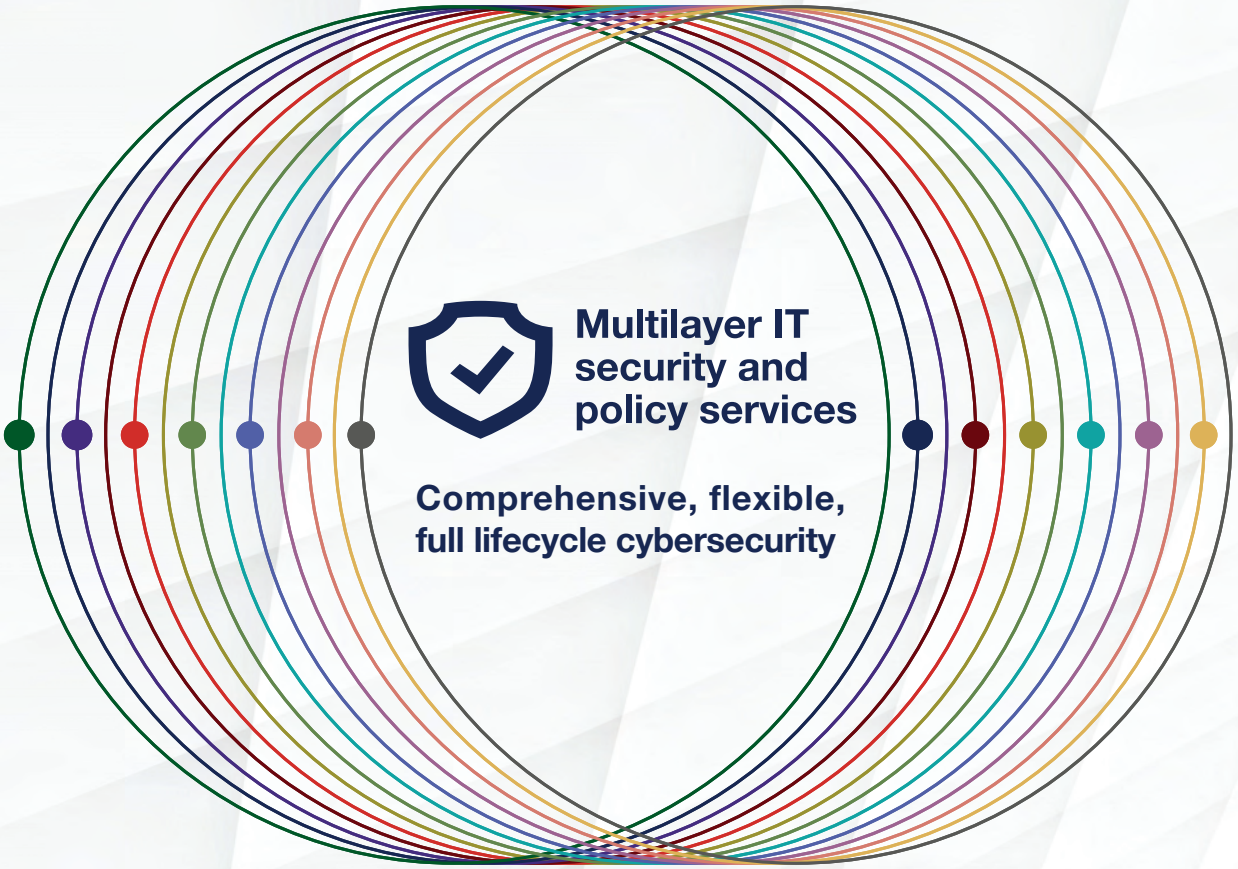
Key cost drivers are included to serve as inputs for pricing. DOJ also provides on-site support outside of the Washington, D.C., area for some services and, in these cases, requires reimbursement for travel costs.

Service metrics

Service metrics assist customers in evaluating DOJ's service, including total activities monitored, budgets, compliance, deliverables, project schedules, and more.

Justice IT Services Offerings

Cybersecurity Services



Additional layers of protection strengthen cyber defense and posture. Add all cybersecurity services to ensure the highest level of protection.

Intelligence Community (IC) and law enforcement partnerships ensure adaptive intelligence and threat detection and prevention.

Services subject to change.

Cybersecurity Operations Services

Security Operation Center (SOC) Services

Monitor networks and systems 24x7x365.

Detect, analyze, and respond to incidents.

Insider Threat Prevention and Detection (ITPD) Services

Deter, detect, and mitigate insider threats.

Receive alerts for malicious or careless activity.

Vulnerability Management

Check databases, operating systems, applications, and endpoints for vulnerability.

Find misconfigurations, weak passwords, unsupported systems and software, and more.

Cyber Threat Hunt Assessment

Proactively search for threats that have already bypassed defenses and established a foothold.

Penetration Testing

Identify exploitable vulnerabilities to determine risk.

Measure compliance with security policies.

Test security awareness of employees.

Anti-Phishing Program Support

Simulate attacks to test employee response.

Measure and train workforce for resiliency to mitigate risk.

Justice Cloud-Optimized Trusted Internet Connection Service (JCOTS)

Resilience

Maintain geographic diversity: East | West

Cloud Optimization

Connect directly to Amazon Web Services, Azure, Box, and Microsoft 365 Office.

Auto Mitigation of Distributed Denial of Service (DDOS)

Continually mitigate network traffic to filter malicious activity.

Governance, Risk, and Compliance Services

Cybersecurity Policy Support

Develop and maintain information security and privacy policies to ensure compliance.

Information System Security Officer (ISSO) Services

Integrate cybersecurity standards into IT system lifecycles.

Independent Security Control Assessments

Assess security controls for Authority to Operate (ATO) recommendations.

Cybersecurity Assessment and Management (CSAM) / Security Posture Dashboard Report (SPDR)

Automate inventory tracking and ongoing authorizations for compliance with the Federal Information Security Modernization Act of 2002 (FISMA).

Leverage SPDR, a premium option, to increase risk visibility and gain insights that improve security posture.

Supply Chain Risk Management (SCRM)

Provide vendor research, risk scoring, and threat information to decision makers.

Cybersecurity Technical Services

Optimize security operations with information security and privacy topics.

Cybersecurity Operations Services

DOJ shields enterprises against threats and strengthens their cyber-defense, enabling them to focus on their mission. Cybersecurity Operations Services provided by Justice IT Service Offerings protects agencies of any size and with industry-leading cyber specialists and technologies. DOJ delivers an unmatched capability to integrate advanced threat intelligence from across the federal government to further enhance an enterprise's security posture.

A standard set of capabilities is offered for each service to meet baseline customer requirements, and optional enhancements are available to deploy additional capabilities at an additional cost. The flexibility of our services assists customers with finding the right solution for their unique needs. Services include:

Security Operations Center (SOC) Services

Insider Threat Prevention and Detection (ITPD) Services

Vulnerability Management

Penetration Testing

Cyber Threat Hunt Assessment

Anti-Phishing Program Support

Security Operations Center (SOC) Services

Description

SOC is a premier service offered by DOJ. The Justice Security Operations Center (JSOC) serves as the nexus for network monitoring, incident response, cross-agency information sharing, threat intelligence, and cybersecurity investigations. JSOC complies with U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) guidelines for SOC shared service providers.

Capabilities are available to all customers using the service, with add-ons and packages available to expand capabilities based on each customer's unique requirements.

Capabilities

Cyber threat intelligence and information sharing – Review and analyze classified and open source threat intelligence to maintain awareness and enhance capabilities, disseminate patch availability for vulnerabilities, and share advisories with customers and other federal specialists.

Network and system monitoring – Provide 24x7x365 monitoring of all networks, systems, and external-facing applications and sites to detect suspicious activity, including:

- **High Value Assets (HVAs) monitoring** – Monitor HVA security to ensure mission-critical systems and data are protected.
- **Event categorization and prioritization** – Categorize, prioritize, and document security events, including incident alerting and sorting for additional investigation.
- **Malware analysis** – Analyze malware through dynamic methods (executing programs in a controlled sandbox) and static methods (manually reviewing malware).

Incident analysis and correlation – Examine incidents to identify the scope and nature of each, the parties involved, the timeframe, correlation to other incidents, and available response strategies.

Incident response – Implement plans, Standard Operating Procedures (SOPs), and communications to handle suspicious events and incidents in coordination with the appropriate stakeholders, including the insider threat program.

Incident management – Manage and document all people, processes, and technologies to handle suspicious events and incidents, continuously improve incident management, and enhance quality and effectiveness, including:

- **Communication and coordination** – Communicate to quickly disseminate the right information to the right people at the right time, and coordinate activities with internal/external parties (e.g., coordinating centers, incident response teams, system owners, and victims, as well as service providers or vendors).
- **Incident closeout and postmortem** – Verify implementation of recommended response activities; assess responses to identify issues or lessons learned, propose improvements, and act on findings or recommendations.
- **Incident archiving and reporting** – Archive incidents and reports in a repository; report incidents to customers and other external organizations in compliance with federal requirements, including dashboards with metrics and trends, as well as providing optional reports to third parties, such as DHS's United States Computer Emergency Readiness Team (US-CERT).

SOC resilience – Ensure continuous operations, including SOC asset management, data protection, and network/systems monitoring of SOC vital functions, providing vulnerability assessment and remediation.

Customer support – Transition customers from current SOC capabilities to DOJ's SOC services, as well as ongoing reporting of service status and resolution of service issues.

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Security Operations Center (SOC) Services
(continued)

Add-ons

Endpoint Detection and Response (EDR) – Combine real-time endpoint monitoring and collection of endpoint data with rules-based automated response and analysis.

Computer forensics – Conduct forensic investigations on affected hardware, including end-user equipment (e.g., laptops, smartphones, etc.), collecting evidence for litigation and evaluating the cause and impact of the intrusion.

Onsite incident response – Incorporate support for malicious, suspicious, or prohibited activities in coordination with customers.

Related services

Customers may include additional services with SOC capabilities to further enhance their security posture. These services also may be acquired as standalone services for customers not leveraging DOJ's SOC capabilities:

Cyber Threat Hunt Assessment

Justice Cloud-Optimized Trusted Internet Connection Service (JCOTS)

Penetration Testing

Vulnerability Management

Cost drivers

Total employees and endpoints

Total network connection sites

Amount of log data ingested

Service metrics

Service availability – Identify the percentage of time without a service outage.

Workload and efficiency – Track the total number of events and incidents.

Incident detection and response – Record the time to detect and respond to each incident.

DOJ protects mission-critical IT systems.

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Insider Threat Prevention and Detection (ITPD) Services

Description

DOJ's Insider Threat Prevention and Detection (ITPD) Services provide the foundation for analytical and investigative capabilities to operationalize an insider threat program. DOJ's ITPD Services enable organizations to deter, detect, and mitigate the risk of insiders using authorized access to resources (equipment, systems, facilities, information, networks, and personnel) to harm—wittingly or unwittingly—national security through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of an organization's resources or capabilities. Based on DOJ's Insider Threat Prevention and Detection Program (ITPDP), a federal leader for insider threat capabilities, and for the National Insider Threat Task Force (NITTF), DOJ's ITPD Services leverage DOJ's skill in establishing and operating insider threat programs.

Capabilities

Program advisory support – Support the development of agency-specific policies and procedures for an insider threat program before providing operational services under that agency's authorization.

Critical Asset Vulnerability Assessments (CAVAs) – Distinguish and assess assets deemed essential to operations, including high-value data and systems (i.e., mission-critical assets, often known as the "crown jewels," the assets of greatest value that would cause major business impact if compromised), personnel, and physical locations.

Data source analysis and configuration – Identify possible data sources, review existing system logging and control requirements for IT data sources, and, if needed, recommend changes to the data sources to support an insider threat program.

Data models, behavioral analytics, and automated alerts – Leverage data models and behavioral analytics to configure automated alerts for malicious or careless activities.

Insider threat identification – Identify threats through two primary channels: tips from the organization's workforce, and the program's analytics and alerts concerning behavior. The insider threat team operates during normal duty hours (i.e., 9:00 A.M. to 5:00 P.M. Eastern Standard Time) to receive

tips via email or phone. A voicemail is provided for off-hours and weekends. When a threat is identified, specialists collect relevant information and collaborate with organizational stakeholders to determine if a thorough inquiry/investigation is necessary.

Intelligence Community (IC) and law enforcement partnerships – Partner with federal law enforcement entities and the IC in order to retrieve specialized data that may provide a more accurate and complete picture of activities associated with an inquiry or investigation.

Investigation support – Perform additional inquiry or information integration and analysis on user activities when requested, and coordinate findings with the relevant customer stakeholders while complying with privacy requirements.

Collaboration and coordination – Collaborate and coordinate with customers' organizational stakeholders, such as general counsel, human resources, and privacy offices, to ensure employee privacy, as well as compliance with organizational policies. Customers retain their responsibility to take action based on the findings of inquiries or investigations.

Cost drivers

Number of employees

Number of data sources

Sophistication of required data models

Data storage and retention requirements

Service metrics

Number of user activities monitored, spanning Unclassified, Secret (S), and Top Secret (TS) levels

Number of alerts or incidents (with breakouts by severity, rule set, and user group)

Alert and incident trends (with breakouts by severity, rule set, and user group)

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Vulnerability Management

Description

DOJ offers both ongoing and ad hoc vulnerability scanning to help customers detect databases, operating systems, applications, Web applications, and endpoints that may be vulnerable to attack and to understand the nature of the vulnerabilities. DOJ does not provide patching or flaw remediation, but DOJ collaborates with customers to ensure the outputs of vulnerability scans support flaw remediation efforts and to provide recommendations for remediation of vulnerabilities.

Capabilities

Vulnerability scanning tools – Leverage industry-leading vulnerability scanning tools configured and maintained for use in the customer's environment.

Vulnerability scanning – Complete credentialed scans at the application (including Web applications, external webpages), middleware (e.g., databases), and endpoints (e.g., hosts, operating systems) layers. DOJ also can conduct non-credentialed scans of Web applications and external webpages if required. Scans identify vulnerabilities, such as:

- Missing patches and updates
- Misconfigurations allowing unintentional data exposure
- Weak and default system passwords
- Unsupported operating systems and software
- Insecure and unnecessary network services

Compliance scanning – Perform automated scanning to analyze and report on the security configuration of an information system using baselines from Security Technical Implementation Guides (STIGs).

Crowdsourced vulnerability disclosure – Conduct continuous vulnerability discovery and assessment of external-facing websites and applications by the general public, including cybersecurity researchers.

Expert analysis and reporting – Analyze scan results, develop reports on vulnerabilities discovered, and provide risk-based recommendations on the disposition of identified vulnerabilities. Provide leadership with graphical representations of vulnerabilities within their respective environments to support decisions for improving security and vulnerability postures.

Service levels

Two service levels are offered:

1) Ongoing vulnerability management

The customer's assets are added to DOJ's enterprise vulnerability scanning platform to continuously scan for security vulnerabilities on connected devices. Multiple scanners, through the Tenable Security Center and Tenable's professional feed of network vulnerability plugins, are employed to detect systems that may be vulnerable to attack, and to report any high-risk vulnerabilities to designated security contacts for investigation and remediation.

2) Ad hoc vulnerability assessment

Scan a single vulnerability, and report the details and recommended remediation(s).

Cost drivers

Number of databases, Web applications, and endpoints in scope

Service metrics

Compliance with project schedules

Percentage of hosts with credentialed scan results

Average age of scan results per host

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Penetration Testing

Description

Penetration testing uses a variety of tactics, techniques, and procedures to identify exploitable vulnerabilities in networks and systems. This testing also measures compliance with organizational security policies, detecting whether staff are aware of security issues, and, ultimately, determining the organization's risk to cybersecurity threats. Specialists certified in penetration testing and ethical hacking perform penetration testing.

Capabilities

Approved Rules of Engagement (RoE) – Perform network mapping and define the list of services available on the network, then document the RoE to guide the scope and activities of the test.

Penetration testing – Complete a variety of penetration tests, based on the system's criticality, the test objectives, and organization's requirements, including:

- Targeted testing – Collaborate with IT personnel to test a carefully defined scope.
- External testing – Mimic outside attackers to determine if access to the system can be gained, and, if so, what information can be accessed.
- Internal testing – Simulate insider attacks to determine the risk employees with various access levels pose to the organization.
- Blind testing – Conduct testing with little information about the target and organization in an attempt to more closely mimic an actual attack. Customers also may choose to make this double-blind by not informing their IT professionals a penetration test is being conducted to further simulate real-word circumstances.

Expert analysis and reporting – Analyze test results, develop a report on vulnerabilities discovered, and provide risk-based recommendations on the disposition of identified vulnerabilities.

Related services

Anti-phishing program support – Run simulated phishing attacks as part of penetration testing, if requested.

Cost drivers

Scope of penetration tests

Methodology used to complete testing

Service metrics

Compliance with defined/established RoE

Compliance with project schedules

Adherence to project budget

Completion of required deliverables

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Cyber Threat Hunt Assessment

Description

Cyber threat hunt assessments proactively search through networks and systems to identify threats that have already bypassed network defenses and established a foothold. Attackers may remain in networks for months, collecting data, searching for confidential material, and moving laterally to execute their objectives. Cyber threat hunt assessments are an essential component of a cyber-defense strategy because many organizations lack the detection capabilities needed to stop these advanced threats from attacking and remaining in the network.

Capabilities

Approved Rules of Engagement (RoE) – Analyze the target organization's mission to develop an assessment of the threat actors most likely to target the organization. Based on research into these groups, DOJ uses detailed information on these attackers' latest Tactics, Techniques, and Procedures (TTPs) to develop a hypothesis for the hunt. DOJ documents the hypothesis, the hunt procedures, and the required tools and data in the RoE, which is approved before initiating the hunt.

Cyber threat hunt execution – Complete the hypothesis-driven hunt using various tools, techniques, and datasets, such as security monitoring tools, Security Information and Event Management (SIEM) data, analytics tools, and user behavioral analysis.

Cyber threat hunt assessment documentation package and briefing – Provide a briefing and documentation package at the conclusion of assessments, including:

- Final approved RoE
- Final report, including the hunt hypothesis, availability of artifacts, findings, and any deployable detection signatures developed during the hunt
- Briefing that describes the results of the hunt

Cost drivers

Scope of the cyber threat hunt assessment

Methodology used to complete the cyber threat hunt assessment

Service metrics

Compliance with RoE

Compliance with project schedules

Adherence to project budget

Completion of required deliverables

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Anti-Phishing Program Support

Description

DOJ provides comprehensive support to establish and operate an anti-phishing program, including employee awareness and training, simulated attacks, and results analysis to inform training modifications and to mitigate the risk of phishing attacks against an enterprise and its workforce.

Capabilities

Program management – Establish a formal anti-phishing program, including operating model, testing objectives and frequency, and Standard Operating Procedures (SOPs).

Simulated phishing attack platform – Configure an anti-phishing platform that enables management of target lists for testing, development of realistic phishing emails, and completion of time-bound campaigns.

Campaign support – Operate regular anti-phishing campaigns to target lists. Campaigns may vary in scope (e.g., offices, divisions), difficulty (realistic vs. obvious), or in type of information elicited (e.g., passwords, document downloads). Campaigns may be developed based on emerging threat intelligence to prepare the organization for a possible attack that has already occurred in another organization.

Dashboards and reporting – Monitor the results of campaigns at the target-level or campaign-level, and analyze results to improve anti-phishing training and communications, and inform future campaigns.

Cost drivers

Number of users

Number of campaigns

Service metrics

Emails distributed

Emails delivered

Employees tested annually

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Justice Cloud-Optimized Trusted Internet Connection Service (JCOTS)

DOJ's Trusted Internet Connection (TIC) service provides a cloud-optimized, secure Internet connection with a modular, scalable design. The direct connection to cloud service providers (Amazon Web Services, Azure, Microsoft Office 365) features minimal latency and high bandwidth, as well as highly resilient U.S. east and west redundancy for continuity of operations.

Justice Cloud-Optimized Trusted Internet Connection Service (JCOTS)

Description

JCOTS securely connects customers to the Internet, email servers, and commercial Cloud Service Providers (CSPs) with a modular, scalable design to protect both on-premise and cloud-based applications. JCOTS offers highly resilient U.S. east and west redundancy for failover capability, providing 99.99% high availability, as well as direct connection to CSPs with minimal latency and high bandwidth.

Capabilities

Trusted Internet Connection (TIC) – Meet and exceed all federal TIC 2.2 requirements using best of breed security technologies.

Cloud optimization – Connect directly to commercial CSPs (Amazon Web Services, Azure, Microsoft Office 365) with minimal latency and high bandwidth.

Redundancy and high availability – Provide full redundancy with geographic and power grid diversity, high availability at 99.99%, and automated failover capacity.

Distributed Denial of Service (DDOS) auto-mitigation capabilities – Automatically identify DDOS network traffic and divert traffic to scrubbing facilities to filter malicious traffic and allow valid traffic.

Secure transport – Secure edge server transport for inbound and outbound email, inbound and outbound Internet traffic (forward and reverse proxy), Domain Name System (DNS) zoning, and remote access.

Malware detection and detonation – Detect, execute, and analyze potential email malware in a sandbox environment.

Intrusion prevention – Detect and prevent malicious traffic targeting government networks with EINSTEIN 3 – Accelerated (E3A) intrusion prevention.

Data loss prevention – Determine potential data breach transmissions and prevent data loss by monitoring, detecting, and blocking sensitive data.

Packet capture – Conduct full packet capture and storage for 120 days to provide investigative capabilities for security specialists and network troubleshooting capabilities for operations teams.

Cost drivers

Number of network sites

Amount of network traffic

Service metrics

Percentage of service time without JCOTS outage

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Governance, Risk, and Compliance Services

DOJ's Justice IT Service Offerings provide advisory services on a wide range of information security and privacy topics, including enterprise program management, process improvement, and optimization of security operations. Services include:

Cybersecurity Policy Support

Information System Security Officer (ISSO) Services

Independent Security Control Assessments

Supply Chain Risk Management (SCRM)

Cybersecurity Assessment and Management (CSAM)

Cybersecurity Policy Support

Description

DOJ assists customers in developing and maintaining information security and privacy policies based on the most recent guidance from legislation, executive orders, directives, policies, regulations, and other technical standards.

Capabilities

Policy development – Create required policies that have not previously been developed in accordance with federal, departmental, and oversight guidance.

Policy review and modernization – Analyze and update existing policies, as well as maintain ongoing updates, based on current and changing federal, departmental, and oversight guidance.

Cost drivers

Labor required to perform the project scope

Service metrics

The number of cybersecurity policies (both, policy updates and policies in development)

Compliance with project schedules

Adherence to project budgets

Quality of work products and deliverables

Information security and privacy policies ensure compliance.

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Information System Security Officer (ISSO) Services

Description

DOJ's ISSO Services help comprehensively integrate cybersecurity into system development lifecycles and comply with the federal government's Risk Management Framework (RMF) standards as maintained by the National Institute of Standards and Technology (NIST). DOJ ISSOs develop and maintain all system security documents, support the assessment and authorization process to ensure the system receives an Authority to Operate (ATO), and provide continuous monitoring to maintain a sound security posture.

Capabilities

System security documentation – Develop and maintain various system security documents, including but not limited to privacy threshold or impact analysis, business impact analysis, system security plans, incident response plans, or contingency plans.

Assessment and Authorization (A&A) support – Generate documents required for the ATO package, coordinate with the assessment team to perform the system's security assessment, and facilitate support to implement any mitigation steps needed to acquire the ATO.

Continuous monitoring – Continuously monitor system security, providing stakeholders visibility into the information system's security status over time, as well as supporting configuration management, security impact analysis on system changes, assessment of selected security controls, incident reporting, and security status reporting.

Plan of Action and Milestones (POA&Ms) – Track POA&Ms, as mandated by the Federal Information Systems Management Act of 2002 (FISMA), that are identified as a result of the security assessment or as an outcome of continuous monitoring activities, and facilitate closure of POA&Ms.

Related services

Cybersecurity Assessment and Management (CSAM) application and Security Posture Dashboard Report (SPDR) – Implement numerous features that assist ISSOs in the efficient completion of required activities.

Cost drivers

Number of systems

Each system's *NIST Federal Information Processing Standard Publication 199 (FIPS-199)* categorization

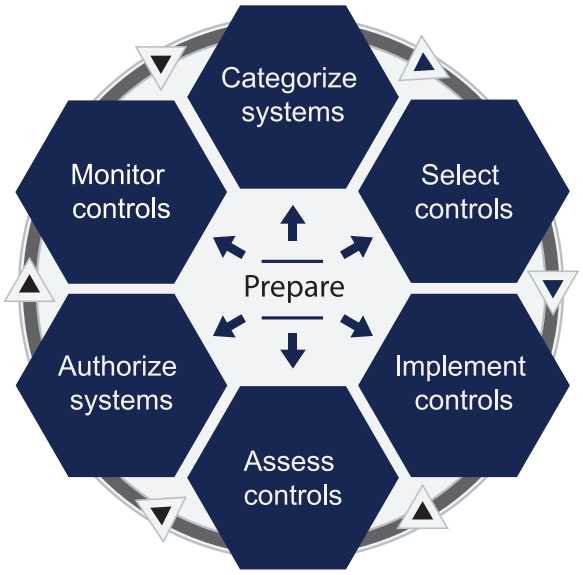
Service metrics

Increase in FISMA scores

Successful ATOs

Resolution of incidents within established timeframes

Risk Management Framework



What is RMF?

RMF is the federal government's mandated information security framework to ensure the security of information systems.

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Independent Security Control Assessments

Description

DOJ's Independent Security Control Assessments uncover more and higher priority risks as part of the Assessment and Authorization (A&A) steps of the Risk Management Framework (RMF). DOJ services provide agencies with an independent assessment of the security controls selected for the system, resulting in a recommendation of whether the system should receive an Authority to Operate (ATO). DOJ's assessment methodology is consistent with the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53* regulations.

Capabilities

Security Assessment Plan (SAP) – Develop a plan based on system documentation, and review the plan with customer stakeholders to confirm the environment and all components are sufficiently covered.

Assessment activities – Perform a variety of assessment activities based on the Special Access Program (SAP) security criteria, including vulnerability scans, visual observations, documentation reviews, and stakeholder interviews.

Security Assessment Report (SAR) and Plan of Action and Milestones (POA&Ms) – Assessors document the results in the SAR upon completing the assessment, providing a prioritized list of risks, mitigation recommendations, and POA&Ms.

Authority to Operate (ATO) briefing and documentation package – Provide a final briefing, including the final recommendation to approve or deny the ATO, and a documentation package of all artifacts and data created or used by the assessment team.

Optional services

High Value Asset (HVA) assessment – Prioritize and secure HVA information systems through tiered assessments:

Tier 1 – Conduct pre-assessments with the same methodology as the U.S. Department of Homeland Security (DHS) to identify and mitigate weaknesses in preparation for the formal Tier 1 assessments performed by DHS.

Tier 2 | Tier 3 – Implement independent security control assessments, as well as policy evaluation, Security Architecture Reviews (SARs), and penetration testing.

Cost drivers

Number of systems

Each system's *NIST Federal Information Processing Standard Publication 199 (FIPS-199)* categorization

Type of system (e.g., general support system, major application, cloud system)

Service metrics

Compliance with project schedules

Adherence to project budgets

Completion of required deliverables

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Supply Chain Risk Management (SCRM)

Description

SCRM helps customers manage information communications and technology supply chain risk by providing vendor research, risk scoring, and threat information to decision makers.

Capabilities

Regulatory and policy analysis – Track supply chain legislation, regulations, and policies from sources, such as the Federal Information Systems Management Act of 2002 (FISMA), National Institute of Standards and Technology (NIST), and United States Office of Management and Budget (OMB) directives to identify impacts to the SCRM program.

Supply chain threat intelligence – Monitor and analyze classified and open source threat intelligence to maintain situational awareness and to ensure emerging threats are properly identified and assessed.

SCRM program management and advisory support – Develop a methodology, including Standard Operating Procedures (SOPs), for completing risk assessments and maintenance of program documentation based on regulatory and policy analysis and threat intelligence.

SCRM assessments – Research and analyze hardware and software acquisitions to identify supply chain risks, including vendor insolvency and litigation, as well as cyber terrorism, malware, data theft, and Advanced Persistent Threat (APT) risks. When DOJ's point-in-time assessment is completed, a summary risk assessment report is provided, including recommendations for risk mitigations.

Reports to Congress – Incorporate assessment findings into DOJ's quarterly summary report to Congress if requested by the agency.

External stakeholder collaboration – Provide quarterly reports and coordinate with government-wide supply chain initiatives, such as the Federal Acquisition Security Council (FASC).

Cost drivers

Number of assessments

Service metrics

Compliance with project schedules

Adherence to project budgets

Completion of required deliverables

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Cybersecurity Assessment and Management (CSAM) and Security Posture Dashboard Report (SPDR)

Description

DOJ's CSAM application enables agencies to automate Federal Information Security Modernization Act of 2002 (FISMA) inventory tracking and ongoing authorization processes, while following the Risk Management Framework (RMF). CSAM is an end-to-end Assessment and Authorization (A&A) application providing automated inventory, configuration, and vulnerability management, along with standard data for use in reports and dashboards. SPDR is a premium option that provides increased risk visibility and insights that drive positive changes to improve agencies' security posture.

Capabilities

Common controls, enhanced inheritance, and automated baselines – Provide robust common control and inheritance capability, combined with business intelligence, to automate baselines defined in *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, NIST SP 800-53,* and *NIST SP 800-60.*

Ongoing authorization and A&A management – Automate System Security Plan (SSP) generation and ongoing A&A processes to support evolving United States Office of Management and Budget (OMB) Circular A-130 and FISMA requirements, and monitor Authorization to Operate (ATO) statuses and resource allocations/budgets.

Plan of Action and Milestone (POA&M) management – Streamline and standardize POA&M processes across the organization to leverage POA&M creation, status workflows, control associations, completion tracking, and notifications.

Robust reporting and dashboards – Generate on-demand reporting with powerful filtering capability, supplemented with a data Application Programming Interface (API), to support audit management, Inspector General (IG) requests, data insight, and data import/export functionality.

Oversight and support – Provide security control assessment organization and efficiencies through control selection and grouping capability (referred to as a "motive"), enabling streamlined assessments and monitoring in support of oversight requirements (i.e., OMB Circular A-123, core controls, privacy, etc.).

Customer support and training – Deliver onboarding support to transition customers to CSAM and ongoing customer relationship management support to provide guidance, gather feedback, and assist in the maturity of the application/customer, as well as training and user forums to support ongoing CSAM proficiency, adoption, and optimization.

Continuous application enhancements – Provide enhancements and improvements that are implemented within continuous releases to maintain alignment with evolving regulations and policies and enhanced application capabilities.

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Optional services

Security Posture Dashboard Report (SPDR) and risk scoring – Identify tailored and actionable outputs, delivering risk visibility and insight to drive positive change by supplementing CSAM A&A data with Hardware Asset Management (HWAM), Software Asset Management (SWAM), Vulnerability Management (VULN), and Secure Configuration Management (SCM) data.

CSAM advisory services – Furnish dedicated on-site support to customers to ensure the application is effectively utilized and continuously aligned with the organization's policy, posture, maturity, and culture.

Cost drivers

Number of systems

Number of users

Number of endpoints

Number of data sources and tools

Scope of advisory services requirement

Service metrics

Application availability/uptime

Service issue response time

Service request response time

Cybersecurity Technical Services

DOJ's Justice IT Service Offerings assess security plans for sufficient regulatory and policy analysis and maintain compliance with legislation, regulations, and policies, while identifying supply chain risks as well as emerging threats and recommended risk mitigations.

Cybersecurity Technical Services

Description

DOJ provides advisory services on a wide range of information security and privacy topics, including enterprise program management, process improvement, and optimization of security operations.

Advisory services

Cyber Defense Posture Assessment / Cyber Readiness Assessment – Highlight capability gaps, identify opportunities for improvement, and provide a prioritized roadmap and transition plan for closing gaps and improving defensive capabilities to achieve the desired future state.

Enterprise program management – Offer Chief Information Security Officer (CISO) advisory services for establishing or optimizing enterprise-level cybersecurity programs.

Process improvement – Review, analyze, and enhance cybersecurity processes to improve quality, reduce costs, and ensure compliance.

Security Operations Center (SOC) optimization – Promote effective and efficient SOC operations by providing advisory services on optimal operating models; practices and processes; and, tools and technologies.

Security architecture and engineering – Provide project-based support for developing or modernizing documentation, such as design documents or architectural reviews.

Custom solutions and security software development – Deliver end-to-end agile software development services to enable cost-effective cybersecurity solutions.

Note: Additional advisory services are available.

Cost drivers

Labor required to perform the project scope

Service metrics

Compliance with project schedules

Adherence to project budgets

Completion of required deliverables

Contact DOJ at JusticeITServices@usdoj.gov to schedule a demonstration or learn more.

Cybersecurity Assessments Index

Overview

DOJ offers multiple types of cybersecurity assessments to detect vulnerabilities, monitor compliance, and identify mitigation strategies that customers can use to improve cyber-defense posture.

Assessment

Description

- Comprehensive support establishes and operates an anti-phishing program, that includes conducting simulated attacks to evaluate susceptibility to phishing threats.

- Proactive searches through customers' networks and systems discover threats that have already bypassed network defenses and established a foothold.

- A variety of tactics, techniques, and procedures identify exploitable vulnerabilities in networks and systems while also measuring compliance with organizational security policies, testing whether staff are aware of security issues, and ultimately, determining the organization's risk to cybersecurity threats.

- Independent assessments uncover more and higher priority risks as part of the Assessment and Authorization (A&A) steps of the Risk Management Framework (RMF). Services provide an independent assessment of the security controls selected for the system, resulting in a recommendation of whether the system should receive an Authority to Operate (ATO).

- Assessments manage information communications and technology supply chain risk by providing vendor research, risk scoring, and threat information to decision makers.

- Scanning detects databases, operating systems, applications, Web applications, and endpoints that may be vulnerable to attack and provides insight into the nature of the vulnerabilities.

Partnership Community

More than 25 agencies and organizations use Justice IT Service Offerings for cybersecurity, including Security Operations Center (SOC) services, as well as Cybersecurity Assessment and Management (CSAM) as an end-to-end Assessment and Authorization (A&A) application. The Information Systems Security Line of Business (ISSLoB) actively shares best practices to create an enhanced information technology (IT) system security and policy experience across the U.S. government. DOJ's partnership is always growing and includes:

Commodity Futures Trading Commission (CFTC)

Consumer Financial Protection Bureau (CFPB)

Court Services and Offender Supervision Agency (CSOSA)

Department of Energy (DOE)

Department of Homeland Security (DHS)

Federal Communications Commission (FCC)

Federal Deposit Insurance Corporation (FDIC)

Federal Retirement Thrift Investment Board (FRTIB)

Federal Trade Commission (FTC)

Internal Revenue Service (IRS)

National Science Foundation (NSF)

Peace Corps

Pension Benefit Guaranty Corporation (PBGC)

Pretrial Services Agency for the District of Columbia (PSA)

U.S. Department of Agriculture (USDA)

U.S. Department of Commerce (DOC)

U.S. Department of Education (ED)

U.S. Department of Housing and Urban Development (HUD)

U.S. Department of Justice (DOJ)

U.S. Department of Labor (DOL)

U.S. Department of the Interior (DOI)

U.S. Department of Transportation (USDOT)

U.S. Office of Special Counsel (OSC)

U.S. Small Business Administration (SBA)

United States Agency for International Development (USAID)

United States Consumer Product Safety Commission (CPSC)

United States Courts

United States Social Security Administration (Social Security)


FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
THRIFT SAVINGS PLAN
1986
U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRETRIAL SERVICES AGENCY
DISTRICT OF COLUMBIA
COMMODITY FUTURES TRADING COMMISSION
1975
UNITED STATES OF AMERICA
CONSUMER PRODUCT SAFETY COMMISSION
SOCIAL SECURITY
USA
ADMINISTRATION
TREASURY
INTERNAL REVENUE SERVICE
DEPARTMENT OF LABOR
UNITED STATES OF AMERICA
UNITED STATES AGENCY
USAID
INTERNATIONAL DEVELOPMENT
ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS
FEDERAL DEPOSIT
1933
INSURANCE CORPORATION
DEPARTMENT OF TRANSPORTATION
UNITED STATES OF AMERICA
DEPARTMENT OF EDUCATION
UNITED STATES OF AMERICA
U.S. DEPARTMENT OF THE INTERIOR
MARCH 3, 1849
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA
UNITED STATES DEPARTMENT OF AGRICULTURE
FEDERAL COMMUNICATIONS COMMISSION
FEDERAL TRADE COMMISSION
UNITED STATES OF AMERICA
MCMXV

Terminology

A&A	Assessment and Authorization
API	Application Programming Interface
APT	Advanced Persistent Threat
ATO	Authority to Operate
CAP	Cross Agency Priority Goal
CAVA	Critical Asset Vulnerability Assessment
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPSC	United States Consumer Product Safety Commission
CSAM	Cybersecurity Assessment and Management
CSOSA	Court Services and Offender Supervision Agency
CSP	Cloud Service Provider
CSPC	Center for the Study of the Presidency and Congress
Cyber QSMO	Quality Services Management Office
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
DNS	Domain Name System
DOC	U.S. Department of Commerce
DOE	Department of Energy
DOI	U.S. Department of the Interior
DOJ	U.S. Department of Justice
DOL	U.S. Department of Labor
E3A	EINSTEIN 3 – Accelerated
ED	U.S. Department of Education
EDR	Endpoint Detection and Response
FASC	Federal Acquisition Security Council
FCC	Federal Communications Commission
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standard Publication
FISMA	Federal Information Systems Management Act of 2002
FRTIB	Federal Retirement Thrift Investment Board
FTC	Federal Trade Commission
GSA	General Services Administration
HUD	U.S. Department of Housing and Urban Development
HVA	High Value Asset
HWAM	Hardware Asset Management
IC	Intelligence Community
IG	Inspector General
IRS	Internal Revenue Service

ISSLoB	Information Systems Security Line of Business
ISSO	Information System Security Officer
IT	Information Technology
ITPD Services	Insider Threat Prevention and Detection Services
ITPDP	Insider Threat Prevention and Detection Program
JCOTS	Justice Cloud-Optimized Trusted Internet Connection Service
JSOC	Justice Security Operations Center
NIST	National Institute of Standards and Technology
NITTF	National Insider Threat Task Force
NSF	National Science Foundation
OMB	United States Office of Management and Budget
OSC	U.S. Office of Special Counsel
PBGC	Pension Benefit Guaranty Corporation
POA&M	Plan of Action and Milestones
PSA	Pretrial Services Agency for the District of Columbia
RMF	Risk Management Framework [See Figure 1 on page 33.]
RoE	Rules of Engagement
S	Secret
SAP	Security Assessment Plan
SAR	Security Architecture Review
SAR	Security Assessment Report
SBA	U.S. Small Business Administration
SCM	Secure Configuration Management
SCRM	Supply Chain Risk Management
SIEM	Security Information and Event Management
SOC	Security Operations Center
Social Security	United States Social Security Administration
SOP	Standard Operating Procedure
SP	Special Publication
SPDR	Security Posture Dashboard Report
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SWAM	Software Asset Management
TIC	Trusted Internet Connection
TS	Top Secret
TTPs	Tactics, Techniques, and Procedures
USAID	United States Agency for International Development
US-CERT	United States Computer Emergency Readiness Team
USDA	U.S. Department of Agriculture
USDOT	U.S. Department of Transportation
VULN	Vulnerability Management

Justice IT Service Offerings

Cybersecurity Services

Contact

Email: JusticeITServices@usdoj.gov
Website: www.Justice.gov/ITServices

About

Justice IT Service Offerings are provided by the U.S. Department of Justice's (DOJ's) Office of the Chief Information Officer (OCIO) and support Cross Agency Priority (CAP) Goals of the President's Management Agenda, including CAP Goal 1: Modernize IT to Increase Productivity and Security and CAP Goal 5: Sharing Quality Services.

These offerings assist the Federal Chief Information Officer, United States Office of Management and Budget (OMB), and the Administrator, General Services Administration (GSA), in executing CAP Goals for information technology (IT) modernization to mitigate risks to data, systems, and networks; implement cutting-edge capabilities; and leverage buying power—while pivoting to modern architectures that improve cybersecurity. DOJ works closely with the Cybersecurity and Infrastructure Security Agency's (CISA's) Quality Services Management Office (Cyber QSMO) to ensure DOJ provides high-quality cybersecurity services that align with federal requirements while reducing costs.

Justice IT Service Offerings enable U.S. government entities to share purchases to reduce costs, share modern technology and experts, and create a central source for certain core services, including cybersecurity, to improve delivery of services to American citizens.

U.S. Department of Justice