Criminal Justice Information Services Division (CJIS)

The FBI's Criminal Justice Information Services Division (CJIS) maintains and enforces the CJIS Security Policy. The intention of the policy is to define standards and objectives that govern access to criminal justice information (CJI). Compliance to the CJIS requirements is not certifiable or auditable for solutions vendors; therefore, there is no official status of "CJIS-certified". There are no official evaluations by third-party auditors or assessors nor does the FBI's CJIS organization assess products or services.

However, iboss can assist organizations beholden to the CJIS Security Policy with the following requirement standards, particularly in security management, availability, encryption, and authentication.

5.3 - Policy Area 3: Incident Response

5.3.2 Management of Security Events

5.3.2.1 - Incident Handling

The iboss Cloud Platform provides a centralized platform that provides threat response and rapid response in support of an organization's internal incident response program.

5.3.2.2 - Collection of Evidence

The iboss platform provides full feature logging and access-controlled retention capabilities vital to support any historical investigation or legal hold. Additionally, log data can be exported in a standardized format for archival.

5.4 - Policy Area 4: Auditing and Accountability

Audit logs are stored within the client's containerized environment. Client administrators can review, investigate, and immediately respond to any anomalous or malicious behavior. The iboss Reporter node delivers advanced event reporting and correlation. Additionally, clients have the opportunity to configure logging directly to their own SIEM environment.

5.4.1 Auditable Events and Content (Information Systems)

Logged data is comprised of user behavioral events (websites visited, data transfers executed), network statistical data, administrative activities, inspection countermeasures (IPS, DLP), and authentication events.

5.4.1.1.1 Content

All required elements are present in the iboss event reporting.

5.4.3 Audit Monitoring, Analysis, and Reporting

Full suite of reporting capabilities included in the platform.

5.4.4 Time Stamps

5.4.5 Protection of Audit Information

The iboss platform provides several levels of administration role-based access controls (RBAC) that limit administrators' authorization to manipulate the system or resulting logs. Client end-users of the platform have no access to any UI on the platform, including the administration portal.

5.4.6 Audit Record Retention

Record (log) retention is fully customizable by client administrators.

5.5 - Policy Area 5: Access Control

5.5.1 Account Management

The iboss platform facilitates a full spectrum of access/account management technologies for client end-users and client administrators. The recommended practice would be to leverage SAML/SSO for all use cases.

5.5.2 Access Enforcement

The iboss platform includes numerous mechanisms and features to control, manage, and inspect access of client end-users to resources (internet, cloud services, and traditional internal solutions) by identity, security posture, geographic location, and other connection features.

5.5.2.1 Least Privilege

The iboss platform empowers entities to enforce least privilege beyond just access to resources. The platform can also provide controls on the activities or actions the user is permitted within a webpage or cloud service.

5.5.2.2 System Access Control

The iboss platform supports and provides multiple options of administrative roles

5.5.2.3 Access Control Criteria

Access control for both the client end-user and the administrative user includes opportunities to apply access based on job assignment/role, physical location, logical location, network address, and temporal conditions.

5.5.2.4 Access Control Mechanisms

Access Control Lists are integrated at various layers of the OSI stack, including groups, machines, and processes.

5.5.3 Unsuccessful Login Attempts

Unsuccessful login attempt controls can be enforced/configured at several layers in the system.

5.5.4 System Use Notification

Administration UI login banner is available and fully customizable.

5.5.5 Session Lock

Reauthentication due to inactivity is employed at the client end-user and administrative UI planes.

5.5.6 Remote Access

The iboss platform can control and manage various remote access technologies. This would include traditional site-to-site VPN and zero trust network access for access to conventional onsite assets for remote users.

5.5.6.1 Personally Owned Information Systems

The iboss platform provides a full array of protections and controls that can be applied to untrusted devices (BYOD). Including system posture verification and Remote Browser Isolation.

5.5.6.2 Publicly Accessible Computers

Client administrators can granularly control remote access and asset identification from any system by enforcing Connectors and client certificates.

5.6 - Policy Area 6: Identification and Authentication

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

The iboss platform integrates with IDPs to provide user-specific identification. This identification is attached to all resultant logs of a user's activities.

5.6.2.1.1 Standard Authenticators

While SAML-based authentication is strongly recommended. The iboss platform supports password complexity that meets or exceeds NIST standards.

5.6.2.2 Advanced Authentication

In addition to SAML and token-based authentication for client end-user access control, the iboss platform also supports client certificates.

5.6.4 Assertions (supporting IDP)

The iboss platform can support a client's current IDP to enforce institution policy.

5.7 - Policy Area 7: Configuration Management

5.7.1.1 Least Functionality

The iboss platform provides granularity and ease of configuration for all features enabling the client administrator to provide least functionality.

5.8 - Policy Area 8: Media Protection

5.8.1 Media Storage and Access

Secure storage and retention controls are entirely client configurable. The platform can even relay logs to an institution-controlled conventional environment and choose not to retain data in the environment. System-level encrypted backups (client-specific keys) are stored in client-specific data repositories within AWS S3 buckets.

5.8.2.1 Digital Media during Transport

The iboss platform provides complete control and customization for data-in-transit encryption. This includes protocols and ciphers.

5.8.3 Digital Media Sanitization and Disposal

Client administrators can choose to purge data from the platform at any time. Additionally, at the conclusion of the engagement, or any time at the client's discretion, all physical media (repositories or drives) related to the client's environment can be forensically deleted with a certificate.

5.9 - Policy Area 9: Physical Protection

The iboss datacenters are located in a secure, manned collocation facility. They are located in cement walled buildings, no windows, no external signage to identify facilities, natural barriers to secure/video protected parking areas. Physical protection is provided by a combined effort of iboss and the collocation partner. Collocation partner provides alarms, fire, water, power, generators, monitoring, video surveillance cameras, and a secure card key with an additional biometric access system. Additionally, all servers are in a secure cage and in locked cabinets with keys distributed only as needed for specific entry and only at the time entry is needed. Servers are locked at the OS level, with all administrators using identifiable, auditable, and privileged IDs. Remote access tools are password protected to add an extra layer of security.

5.10 - Policy Area 10: System and Communications Protection and Information Integrity

The iboss platform enables profound client control over information flows and boundary protections for both client end-users and traditional infrastructure. The Connector application can enforce encryption on data-in-transit that may not otherwise be encrypted, the Zero

Trust Network Access feature can secure identity-based user access to servers or services hosted in a traditional datacenter, the Remote Browser Isolation can secure the activities of a untrusted user or machine to cloud based services.

5.10.1 Information Flow Enforcement

5.10.1.1 Boundary Protections

5.10.1.2 Encryption

5.10.1.2.1 Encryption for CJI in Transit

5.10.1.2.2 Encryption for CJI at Rest

All service-related data (which could conceivably contain CJI) is encrypted at rest.

5.10.1.2.3 Public Key Infrastructure (PKI) Technology

Client certificates can be used at the cloud nodes.

5.10.1.3 Intrusion Detection Tools and Techniques

The iboss platform provides intrusion protection and detection controls.

5.10.1.5 Cloud Computing

Client iboss node environments can be localized to the United States.

5.10.3.1 Partitioning

Management and service delivery planes are wholly separate.

5.10.4 System and Information Integrity Policy and Procedures

Client user mobile devices are supported through embedded proxy functionality. An automatic proxy configuration script sometimes called a PAC file, is used to configure mobile device web proxy traffic to the appropriate iboss gateway node. A “Connector” app is deployed to all scoped assets that facilitate the proxy functionality on remote devices, including mobile devices.

5.10.4.2 Malicious Code Protection

5.10.4.3 Spam & Spyware Protections

5.10.4.5 Information Input Restrictions

5.11 - Policy Area 11: Formal Audits

The iboss platform is designed to securely connect any user (trusted or untrusted) to any application or service. The platform supports successful institutional audits with the full suite of logging and reporting available to client administrators.

5.12 - Policy Area 12: Personnel Security

5.12.2 Personnel Termination

When configured with SAML/SSO (as recommended), the iboss platform will deprovision automatically.

5.12.4 Personnel Transfer

Personnel transfers will inherit permissions from group membership if the platform is configured to leverage domain membership groups.

5.13 - Policy Area 13: Mobile Devices

Client user mobile devices are supported through embedded proxy functionality. An automatic proxy configuration script sometimes called a PAC file, is used to configure mobile device web proxy traffic to the appropriate iboss gateway node. A “Connector” app is deployed to all scoped assets that facilitate the proxy functionality on remote devices, including mobile devices.

5.13.4.2 Malicious Code Protection

5.13.4.3 Personal Firewall

5.13.7 Identification & Auth

5.13.7.2 Advanced Auth (connector auth)

5.13.7.3 Device Certificates

About iboss®

iboss is a cloud security company that enables the modern workforce to connect securely and directly to all applications from wherever they work. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, RBI, CASB and data loss prevention to all connections via the cloud, instantaneously and at scale. This eliminates the need for traditional network security appliances, such as VPNs, firewalls and web gateway proxies, which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss Cloud Platform to support their modern workforces, including a large number of Fortune 50 companies. To learn more, visit www.iboss.com

+1 877.742.6832
sales@iboss.com

101 Federal St
Boston, MA 02110