

IOT Solution Architecture & Implementation and Operational Security - 2022

Who We Are:

We are a multi-department team comprised of two groups, Solution Architecture & Implementation and Operational Security. Solution Architecture & Implementation is a solutioning and implementation team that helps agencies find and implement the right technology solutions to fit business needs while maintaining cohesiveness with other State technologies. Operational Security administers and maintains technology used throughout the State that ensures security, availability, and operability.

Our Mission:

To provide secure, reliable, and integrated technology solutions to our partner agencies so they can better serve our mutual customer, the Hoosier taxpayer.

Department: 493029

Manager: Erik Winblad

What We Do:

Solution Architecture & Implementation

The Solution Architecture & Implementation team is a dedicated support team that helps agencies on new server application installs and projects from start to finish. This provides the same technical team that you can reach out to anytime for your application install project. They assist with being that point of contact for all questions and will engage other IOT team's when needed. The Solution Architecture & Implementation team works closely with the projects that come from the IOT Project Success Center.

Operational Security

The Operational Security team manages more than 7,500 certificates and URLs on the State's proxy. The team also works with the security team to figure out operationally how to resolve configuration on servers to meet compliance requirements. They are also responsible for windows patching, geo-blocking, and IP intelligence on the proxy.

Our Tools:

ASM	Ticket Management and SLA Measurement.
F5/BigIP	Load balanced proxies combine high-speed load balancing and content switching, data compression, content caching, SSL acceleration, network optimization, application visibility, and application security on a single, comprehensive platform.
Cloudflare	Public-facing edge protection that includes WAF services, DDoS protection, Bot protection, and more. Cloudflare provides external DNS record services for the State. Additionally, IOT employs Cloudflare Access to make internal applications securely available externally.
DigiCert	Secure Certificate Provider
SCOM	System Center Operations Manager provides alerts and performance metrics.
SCCM	Server configuration and management.
Secret Server	Password management.
EPM	Enterprise Privilege Manager

Our Metrics:

Mon-Fri 6am-6pm excluding state holidays

Resolve customer issues within 40 IOT business hours: 90%+ G; 87%+ Y; <87% R

Our Customers:

Executive Branch, Attorney General, Judicial Branch, and Secretary of State.

Our Budget:

\$6 million (funded by Server Administration)

Our Growth:

Via a recent rebalancing of teams, the Operational Security team has grown to include ownership of the SCCM and SCOM tools. The Solution Architecture & Implementation team has remained steady, continuing to deliver solutions for all state agencies that IOT services.

Recent Major Accomplishments:

More than 100 agency applications deployed last year.
Improved protected zone standards and process.
Improved Automated server configuration process.
Self-service geo-blocking and IP intelligence portal.