

IOT ISOaaS Program - 2020

Who We Are:

ISOaaS, or Information Security Officer as a Service, is a new program established in July of 2019 by IOT. The program provides a part-time information security resource to agencies that do not have a CISO. Once an MOU is established between an interested agency and IOT, the agency will receive a seasoned information security resource for a predetermined number of hours each week.

Our Mission:

To help agencies in maturing their information security program

Department: 493003

Manager: Bill Woolsey

Formed: July 2019

What We Do:

Consulting with agency management and business leaders in order to understand agency mission drivers and business priorities; legal and regulatory requirements; cybersecurity awareness and additional training needs; current cybersecurity practices and agency-specific threats/limitations; and overall risk comfort levels.

Assessing agency maturity; advising agency on cybersecurity maturity level gaps that are identified in information security risk assessments; comparing gaps with agency objectives as well as with legal and regulatory requirements; and helping the agency develop a prioritized cybersecurity plan that addresses gaps and draws upon mission drivers;

Reviewing information security risk assessments (ie penetration and vulnerability tests);

Assisting agency in the development of cost/benefit analyses of its cybersecurity efforts and explaining the risks associated with particular actions and decisions;

Acting as a liaison between agency 's information security team and its IT, compliance, audit, legal, and human resources management teams;

Informing agencies of IOT capabilities. Recommending projects for IOT involvement that meet a certain complexity threshold (as determined by an IOT project complexity assessment). The parties understand that the agency will be required to pay normal project manager fees in these cases.

Guiding and educating agency management and business leaders concerning cybersecurity risks and recommending best practices and existing (or affordable) tools to help the agency achieve its information security priorities.

Bringing the agency perspective to IOT for security related initiatives and decisions.

The agency is ultimately responsible for its own cybersecurity decisions and owns the risk for their agency. The agency will make its agency head, chief of staff, or top-ranking IT executive available to meet with the resource on a weekly basis to serve as the main point of contact in the reporting structure. The agency must ensure that senior management is committed to the security program.

Our Products:

1212 Security Officer as a Service

Our Metrics: IOT's metrics, NIST CSF (Cyber Security Framework)

Our Customers: State agencies that execute an MOU for the product

Major Accomplishments:

- Helping agencies understand and address compliance requirements
- Driving remediation of vulnerabilities
- Making improvements that will improve 2020 Executive Branch Readiness and NIST CSF maturity assessment scores

Current Projects:

- Developing application specific scanning and penetration testing capabilities.
- Writing ISOaaS Playbook and Control Handbook (guides for future ISOs)
- Adding NIST Privacy Framework to the program