



# mission multiplier

## ISSO-as-a-Service Program

**The Best Value for your Cybersecurity Needs**

**Why pay \$150k or more a year to hire an ISSO? Our ISSO-as-a-Service keeps you compliant and operating smoothly at a fraction of the cost.**

*This document contains Mission Multiplier Consulting LLC Proprietary and Confidential Business Information.*

## The Necessity of an ISSO

The term ISSO, or Information Systems Security Officer, continues to gain prominence the closer we get to December 31, 2017. This is due in part to DFARS 252.204-7012 and NIST 800-171, interconnected government regulations that deal with the protection of Controlled Unclassified Information (CUI) in non-federal information systems and organizations. If you are a federal contractor holding such information, you are subject to:

- **DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting<sup>1</sup>:** “To safeguard covered defense information *contractors/subcontractors must implement NIST SP 800-171*, [emphasis added] Protecting CUI in Nonfederal Information Systems and Organizations, as soon as practical, but not later than Dec 31, 2017. For contracts awarded prior to 1 Oct 2017, contractors/subcontractors shall notify DoD CIO within 30 days of contract award of any NIST SP 800-171 security requirements not implemented at the time of contract award.”
- **The Risk Management Framework (RMF):** As prescribed in *NIST Special Publication 800-37<sup>2</sup>*, RMF replaced DoD Information Assurance Certification and Accreditation Process (DIACAP) as of March 12, 2014. NIST states that “The guidelines in this publication are applicable to all federal information systems other than those systems designated as national security systems,” and that “State, local, and tribal governments, *as well as private sector organizations* [emphasis added] are encouraged to consider using these guidelines, as appropriate.” This means that many private contractors handling government data are subject to the continuous “[...] six-step RMF [that includes] security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring.”

Simply put, if you are a federal contractor or subcontractor, you must implement the requirements associated with these regulations in order to continue doing business with the government. In order to accomplish this, organizations are placing these responsibilities on one individual: an ISSO. However, the costs of employing an ISSO are considerable.

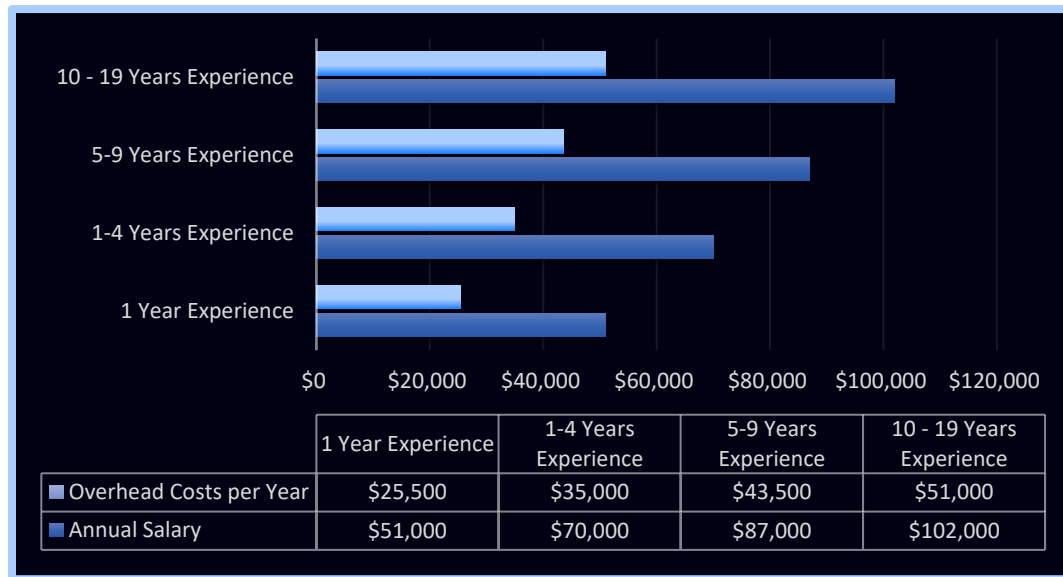
With the DFARS 252.204-7012 requirement deadline looming, Information Systems Security Officers are now as necessary to continued business operations as accountants and lawyers. And we believe that, much like accountants and lawyers, it is usually more cost-effective for small- to medium-sized businesses to outsource this work.

An ISSO handles crucial cyber functions to ensure continued business operations such as:

- establishing appropriate standards and controls
- managing security technologies
- directing the establishment and implementation of policies, plans, and procedures
- responding to incidents
- continuous monitoring of security controls

- ensuring compliance with industry and governmental regulations and laws such as DFARS and RMF

For many businesses, these functions must be fulfilled, but do not necessitate an in-house ISSO to work on a full-time basis. To compound that, the costs of outright hiring an ISSO can be staggering (Figure 1):



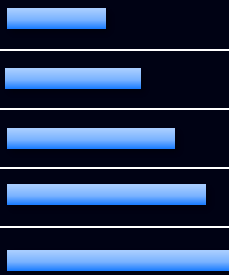
**Figure 1: Cost of an In-House ISSO<sup>3</sup>**

Figure 1 assumes an overhead rate of approximately one-half of the salary of an employee who is a Certified Information Systems Security Professional (CISSP). The reasoning behind these figures is detailed in the following.

*While the price of our ISSO-as-a-Service will vary dependent upon client needs and situation, the following pages should make it extremely evident that our cost will be much more inexpensive than hiring even a novice security professional.*

## Costs Associated with Hiring a Certified ISSO

The cost of hiring an in-house ISSO is probably the ultimate consideration for your organization. The direct salary costs of a certified cyber professional capable of acting as an ISSO vary due to individual industry experience and job location, but according to [glassdoor.com](https://www.glassdoor.com)<sup>4</sup>, the national average salary of an ISSO is \$98,000, with a range of \$59,000 to \$133,000, based on 40 salaries submitted anonymously to Glassdoor by ISSOs at companies such as Raytheon and Boeing. This falls in alignment with research by [infosecinstitute.com](https://www.infosecinstitute.com)<sup>3</sup>, which found that salaries for CISSPs typically range from \$54,820 to \$152,311 nationally. It is important to note that the salaries at the lower end of the spectrum are for CISSPs with less than one year of experience. For those with a mere one to four years' experience, that number jumps to \$69,899. Experience of five to nine years reaches \$87,005, and ten to nineteen comes to \$102,591 (see Figure 2).

Years of Experience	National Mean CISSP Salary
Less than 1 year	\$51,244 
1-4 years	\$69,899
5-9 years	\$87,005
10-19 years	\$102,591
20+ years	\$117,291

**Figure 2: 2017 CISSP Mean Salary by Years Experience<sup>3</sup>**

Beyond simple salary, though, are the administrative and overhead costs associated with hiring and maintaining an upper-level employee. These include usual costs like Workers' Comp, Social Security, 401ks, etc. Other costs associated specifically with an ISSO include continuing education packages, certification fee reimbursement, and other fringe benefits necessary to keep an employee with such a sought-after skillset. Again, Figure 1 uses the rule of thumb of estimating one-half of the employee's salary for their overhead costs.

## Necessity of an ISSO Who Is Industry Certified

We believe that the ISSO for your organization, whether in-house or contracted-out, should be industry certified. Certification shows a common foundation of knowledge and provides proven experience. All of our on-demand ISSOs hold industry certifications such as Certified Information Systems Security Systems Professional (CISSP).

Not all certifications are created equal. While you might consider having someone only holding the CompTIA Security+ certification act as your ISSO, higher-level certifications signal higher levels of experience and knowledge. For example, the CISSP designation has long been considered the gold standard<sup>5</sup> of information security. This is due to CISSP being the first information security certification to be accredited under ISO/IEC Standard 17024 back in June 2004. This longevity has given it world-wide recognition. Professionals with the CISSP designation also must meet rigorous standards in terms of testing, work history, and continuing education in order to obtain and hold it. While some ISSOs may be content to hold a lesser certification, we believe that your company deserves an ISSO that holds the highest standard in the industry.



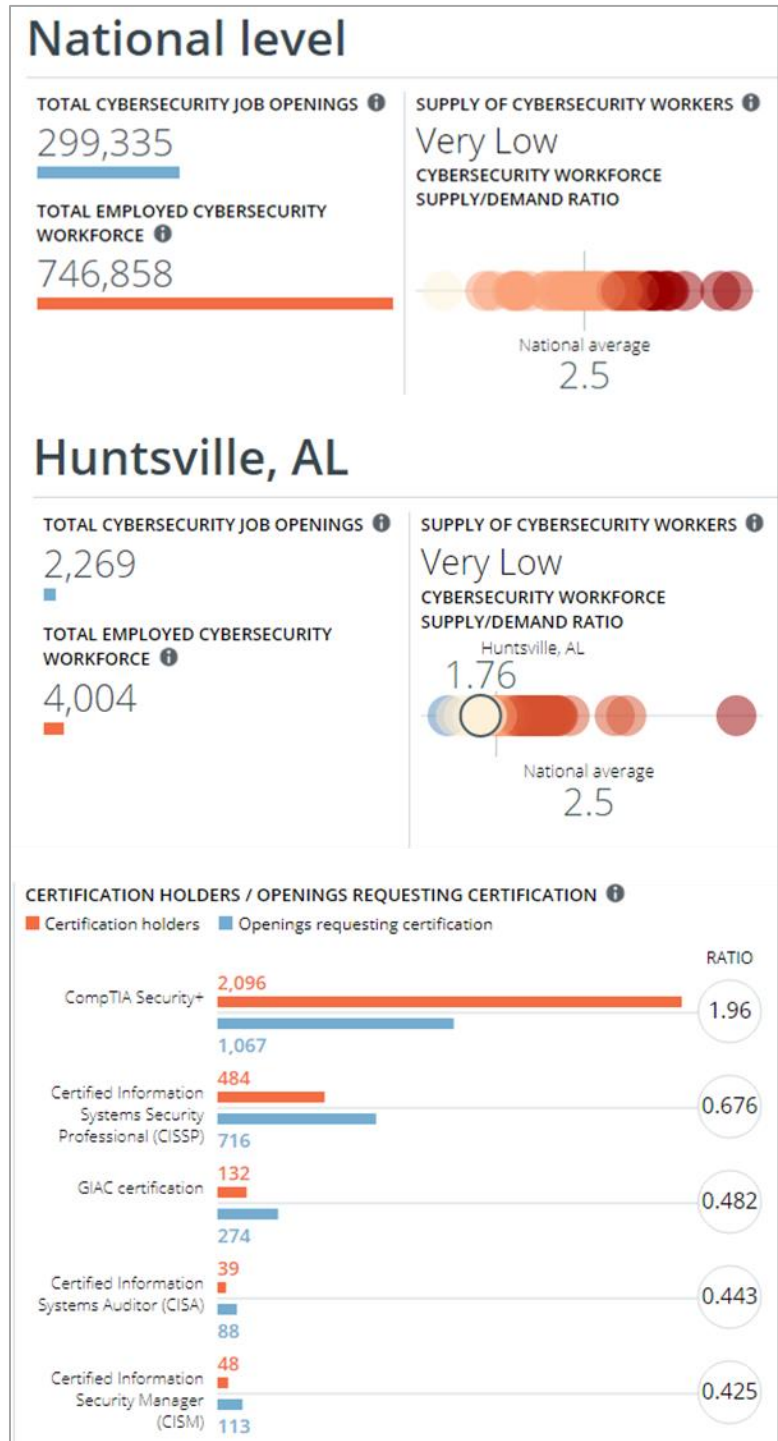
## Availability of Certified Professionals

Even if you decide that you are willing to hire your own CISSP as your ISSO, your company may run into some difficulties just finding one. According to CyberSeek.org<sup>6</sup>, there are nearly 300,000 job openings for cyber security professionals nationwide (see Figure 3, top).

And when the Huntsville Metro Area is examined, the prospect of you finding your own qualified professionals looks even bleaker (see Figure 3, middle).

In Huntsville alone, there is a demand for over 2,000 cybersecurity professionals that simply isn't being met. At the same time, Huntsville's demand for professionals with upper-level certifications like CISSP and CISM shows a marked deficit (see Figure 3, bottom).

Our ISSO-as-a-Service Program can serve as an effective and convenient alternative to fighting your competition over qualified individuals to meet your ISSO needs.



**Figure 3: Cybersecurity Employment Deficits<sup>6</sup>**

## Turnover and Retention

As mentioned, the demand for qualified cyber professionals is fierce. With a dearth of qualified candidates pushing wages up, job hopping is a mainstay in the industry. According to Infosecurity Magazine<sup>7</sup>, "High Cybersecurity Staff Turnover is an 'Existential Threat'". Their findings state that:

*"[...] about 46% of cybersecurity professionals said they are solicited to consider other cybersecurity jobs (i.e. at other organizations) at least once per week. In other words, cybersecurity skills are a sellers' market, where experienced professionals can easily find lucrative offers to leave one employer for another."*

Our ISSO-as-a-Service outright eliminates this negative situation for our customers. While Mission Multiplier is also subject to turnover, our reason for being in business is cybersecurity. Nothing short of full closure of the business will stop us from having certified experts on staff to act as ISSOs.

## Continued ISSO Training and Recertification

Even the most dedicated cybersecurity professional can become so consumed with day-to-day operations that they become distracted from necessary personal functions like completing requisite continuing education and recertification. Companies often have to expend administrative efforts to ensure that their cyber professionals are minding their continued requirements. With ISSO-as-a-Service, it is our responsibility to ensure the on-going requirements of our staff, thus taking the burden off of our clients.

## This Is Our Specialty

We have already come across firms who are within the IT sphere (such as IT technicians and for-profit training centers) who claim to offer "compliance services" that are in fact one-and-done policy templates. They do little, if anything, in the way of custom policy creation, in-depth vulnerability scans, and (most importantly) continued user support throughout the entire process of government inspections/audits and beyond.

Already, some companies have been tempted by cheaper program packages that have very little substance to them. While more thorough services such as ours may appear to be more expensive at first glance, the fundamental integration of specialists who will be there for you in the long-term makes them the more cost-effective option.

## Rating Enhancements

According to the *Manual for the Certification and Accreditation of Classified Systems under the NISPOM*<sup>8</sup>:

*"If the ISSM is not technically competent to securely configure the systems under his or her purview, there must be a local ISSO that can configure and manage information systems to verify their controls are in place and operating in accordance with established policies."*

*During onsite validation visits and security assessments, DSS staff will verify that the ISSM is trained to a level commensurate with the overall complexity of the systems [emphasis added], or that the ISSM has appointed a technically knowledgeable local ISSO."*

While this is intentionally vague, it shows that appointed ISSOs must have a baseline level of training "commensurate with the overall complexity of the systems."

Additionally, it has come to our attention that our clients can receive rating enhancements or "bonus points" on their compliance evaluations based on their ISSO's professional certification levels being above this baseline. Our intelligence indicates that rating enhancements can be gained when:

*"Security staff training exceeds NISPOM and DSS requirements and incorporates that knowledge into NISP administration. Intent of this category is to encourage security program's key personnel to actively strive to learn more and further their professional security expertise beyond mandatory requirements."*

Considering this, your company can gain a *distinct advantage* by showing evidence of how the ISSOs that we provide go above and beyond. This evidence will take the form of certification transcripts and certificates. The holding of multiple upper-level certifications may help your company achieve higher marks on your assessments. The upper-level certifications of our professionals include:

- Information Systems Security Architecture Professional (CISSP-ISSAP)
- Certified Information Systems Security Professional (CISSP)
- Certified Chief Information Security Officer (C|CISO)
- Certified Hacking Forensics Investigator (CHFI)
- Certified Network Defense Architect (CNDA)
- EC-Council Certified Security Analyst (ECSA)
- Certified Ethical Hacker (CEH)

Rating enhancements can also be had by way of specialized employee training via sponsored events:

*"In addition to the annual required security refresher briefings, the cleared contractor holds company sponsored events such as security fairs, interactive designated security focused weeks, security lunch events, hosting guest speakers on security related topics, webinars with the security community, etc. Intent of this category is to encourage cleared contractors to actively set time aside highlighting security awareness and education. This should not be a distribution of a paper or email briefing, but rather some type of interactive in person activity."*

Mission Multiplier can facilitate such events using our strategic partners. These events are engaging, interactive, and can be performed at your location to educate your employees to the latest cyber threats and best practices.

## The Complete Package

We plan on sticking with our clients for the long-term. Our ISSO-as-a-Service Program includes the following continuous benefits for your company (see Figure 6):

1. **Increased Cost Savings:** As previously established, the cost of accessing our on-demand, seasoned ISSOs is significantly less than hiring a full-time cybersecurity professional.
2. **Access to an On-Demand ISSO:** Our highly qualified IT security professionals are fluent in cyber requirements. We know more about regulatory and policy requirements than an average IT technician.
3. **Continuing Maintenance:** We ensure that the appropriate cybersecurity controls are in place to satisfy evolving cyber compliance mandates. While some companies may offer an inferior, one-time package, we stick with our clients, ensuring that they *remain compliant in perpetuity* for their continued benefit.
4. **Cyber Awareness and Training:** We provide cybersecurity awareness training to client staff. As every cybersecurity professional is well aware, human beings are the weakest link in any cyber defense ecosystem. A well-trained workforce will reduce risk.
5. **Mitigating Evolving Threats/Risks:** A huge value over one-and-done cyber companies is that our continued services include staying abreast of the newest cyber threats and being proactive to stay one step ahead. We can oversee and review critical information security systems on a weekly, monthly, quarterly, or annual basis.
6. **Refining Cyber Policies & Procedures:** Many organizations do not have the simplest of contingency plans or user policies in place. Not only can we create such policies for our clients, we can ensure that cyber policies are up to date and in alignment with the organizational mission in perpetuity.
7. **Cloud Expertise:** The vast majority of our clients are fully integrating the cloud into their systems. Clients see the benefits in transferring risk to outside cloud providers. As such, we offer expertise securing cloud infrastructures by using industry best practices and the latest government regulations.





**Figure 4: Mission Multiplier's ISSO-as-a-Service**

## Conclusion

Bottom Line: ISSO-as-a-Service is and will continue to be the best value for your organization's cybersecurity needs. This is because:

1. We take on the vital roles and responsibilities of an in-house ISSO while ensuring compliance with emerging mandatory requirements and policies set down by government agencies and industry.
2. Our ISSO-as-a-Service Program is superior to hiring your own in-house ISSO in terms of 1) cost, 2) scarcity of certified ISSOs, and 3) our industry expertise being leveraged to your benefit (vast number of certifications, in depth experience in all cybersecurity domains, etc.).

The cybersecurity requirements of your organization are expanding at an extremely rapid pace. Mission Multiplier stands ready to meet these needs with our unique approach: ISSO-as-a-Service.

## About Mission Multiplier

Mission Multiplier is a proven Information Technology Consulting firm focusing on cybersecurity, with over three and half years of experience bringing innovative and tailored cybersecurity solutions to government and commercial clients. We are a rapidly growing HUBZone certified small business, recently recognized as formal DoD protégé company – sponsored by MDA’s mentor-protégé program. We were recently nominated as Small Business of the year by the Huntsville / Madison County Chamber of Commerce, and have been bestowed by a number of recent industry awards. We provide the full suite of cybersecurity services – to include planning, engineering, operations, governance, and enterprise IT penetration testing – with a focus on ISSO-as-a-Service.

Mission Multiplier Consulting LLC  
201 Eastside Square, Suite 2  
Huntsville, AL 35801  
[www.missionmultiplier.com](http://www.missionmultiplier.com)



## Mission Multiplier Points of Contact



**Jamie Miller**  
*President / CEO*

201 Eastside Sq, Ste. #2  
Huntsville, AL 35801

256-829-8859 (Office)  
202-390-8919 (Mobile)  
[jmiller@missionmultiplier.com](mailto:jmiller@missionmultiplier.com)



**Jason Hough**  
*Senior Consultant*

201 Eastside Sq, Ste. #2  
Huntsville, AL 35801

256-665-7731 (Mobile)  
[jhough@missionmultiplier.com](mailto:jhough@missionmultiplier.com)

## References

1. “DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.” Department of Defense, URL: [www.delawareptac.org/wp-content/uploads/2017/08/DFAR-252.204-7012.pdf](http://www.delawareptac.org/wp-content/uploads/2017/08/DFAR-252.204-7012.pdf)
2. “Guide for Applying the Risk Management Framework to Federal Information Systems.” NIST, Feb. 2010, URL: [nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf)
3. “Average CISSP Salary 2017.” InfoSec Resources, 6 Jan. 2017, URL: [resources.infosecinstitute.com/average-cissp-salary-2013/#gref](http://resources.infosecinstitute.com/average-cissp-salary-2013/#gref)
4. “Salary: ISSO.” Glassdoor, URL: [www.glassdoor.com/Salaries/isso-salary-SRCH\\_KO0,4.htm](http://www.glassdoor.com/Salaries/isso-salary-SRCH_KO0,4.htm)
5. CertKiller. Is CISSP certification the Gold standard in the industry?, URL: [www.certkiller.com/guide-is-cissp-certification-the-gold-standard-in-the-industry.htm](http://www.certkiller.com/guide-is-cissp-certification-the-gold-standard-in-the-industry.htm)
6. “National level.” Cybersecurity Supply And Demand Heat Map, URL: [cyberseek.org/heatmap.html](http://cyberseek.org/heatmap.html)
7. Tara Seals. “High Cybersecurity Staff Turnover is an 'Existential Threat'.” Infosecurity Magazine, 6 Oct. 2016, URL: [www.infosecurity-magazine.com/news/high-cybersecurity-staff-turnover/](http://www.infosecurity-magazine.com/news/high-cybersecurity-staff-turnover/)
8. “Manual for the Certification and Accreditation of Classified Systems under the NISPOM, Version 3.2.” Defense Security Service, Office of the Designated Approving Authority, 15 Nov. 2013, URL: <http://www.dss.mil/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf>

**Why pay \$150K or more a year to hire an ISSO? Our ISSO-as-a-Service keeps you compliant and operating smoothly at a fraction of the cost.**



Mission Multiplier Consulting LLC  
201 Eastside Square, Suite 2  
Huntsville, AL 35801  
<http://www.missionmultiplier.com>