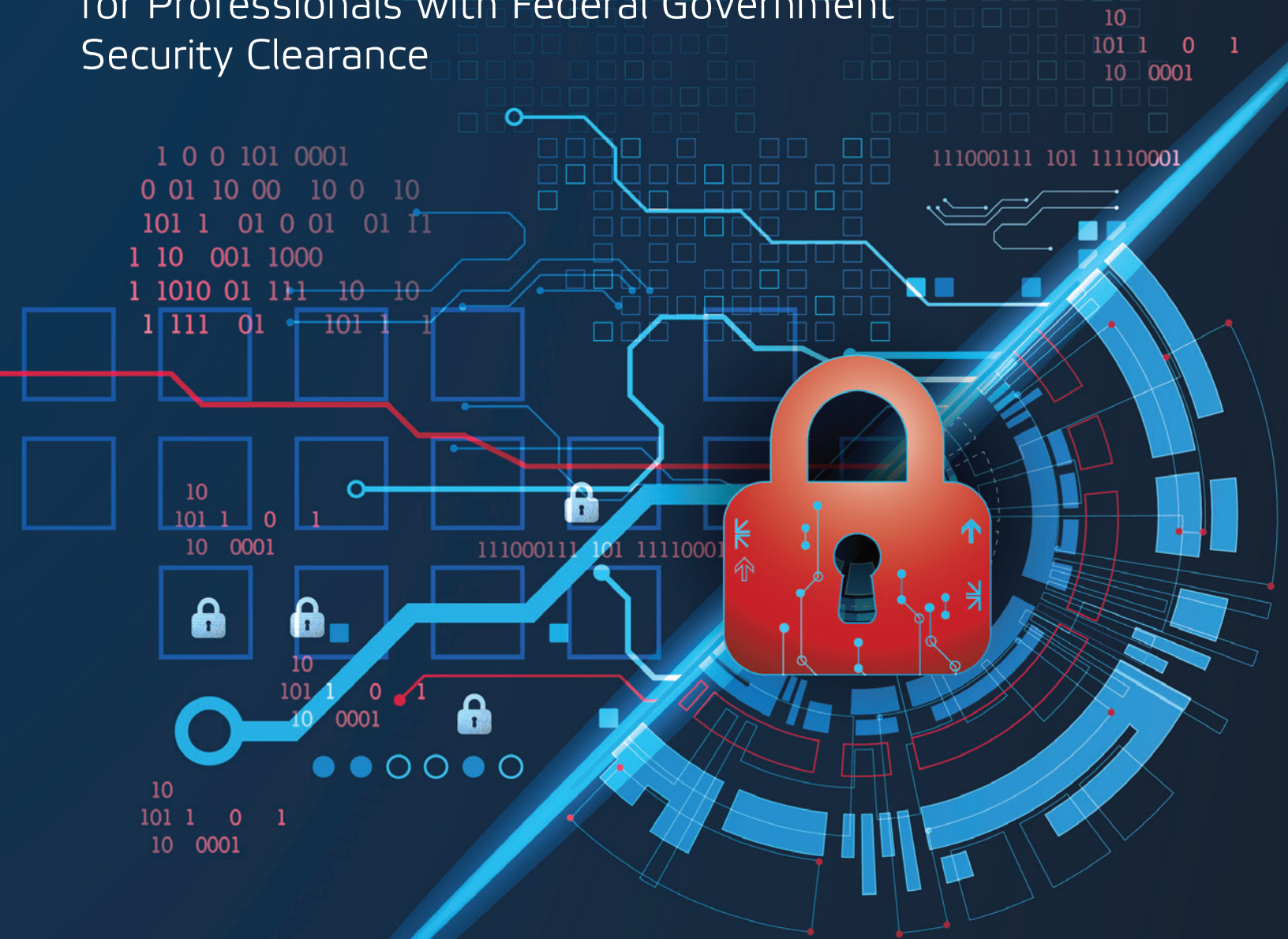


CLEARANCEJOBS

STATE OF THE FACILITY

SECURITY OFFICER 2024

ClearanceJobs is the **Largest Community**
for Professionals with Federal Government
Security Clearance



STATE OF THE FACILITY SECURITY OFFICER

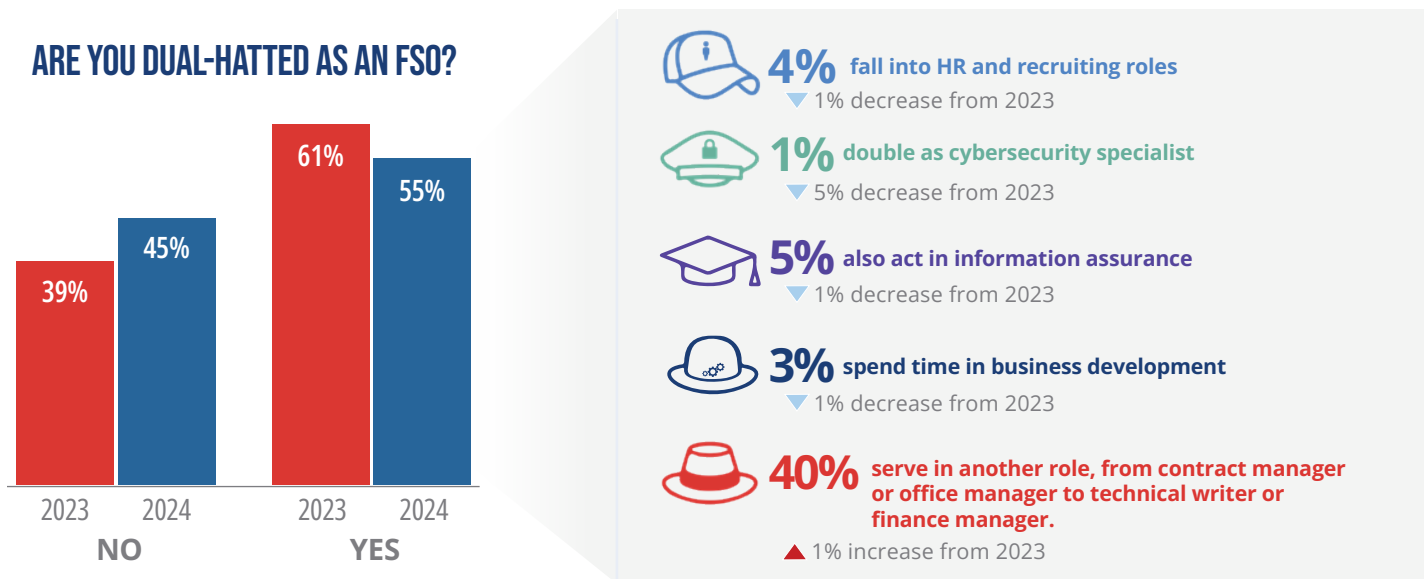
Security officers are the backbone of every national security organization. Often the unsung heroes keeping both classified information and proprietary information safe, they play a vital – and required – role in any National Industrial Security Program (NISP).

With three years of data under our belts, it's clear that many of the trendlines for security officers are a constant, from CUI and personnel security headaches to the benefits of peer networks. Self-reporting ticked up as a topic generating a lot of questions from cleared personnel. Slightly more are using third parties for security training.

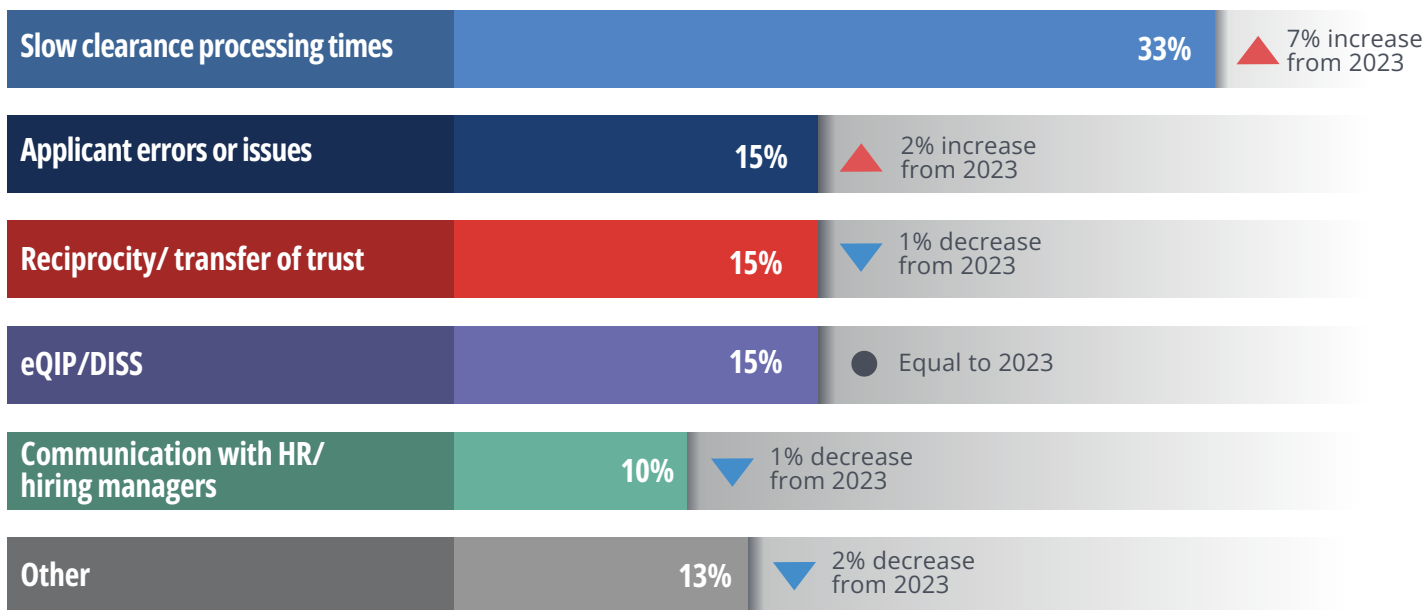
Fortunately, more security officers report having the technology necessary to do their jobs. Compared to last year, no respondents noted using a paper system to track their security-cleared population. While paper didn't get a mention, manual reporting often did. The majority of respondents still note using Excel or spreadsheets, which demonstrates that the methods for tracking are highly variable and rest largely on the shoulders of a single FSO knowing where to find the right documentation. With CUI potentially creating even more for an FSO to have to track, now is the time for security offices and organizations to begin investing in technology and solutions.

The costs of a compromise remain high, and the need for competent security professionals to enforce a proactive security posture great. The survey noted a slight increase in entry-level security officers, but with approximately a quarter of respondents saying they don't have the cleared staff necessary to do their missions, it's clear that security, like the rest of the national security workforce, continues to need to attract the next generation to help it accomplish the mission.

Fewer FSOs say they're dual-hatted into other roles. For those who are, there are fewer with additional technical roles, but many are doing a combination of many functions. The most common areas for FSOs to list as additional roles are ones that fell into the 'other' category, including Insider Threat Program Senior Official (ITPSO), COMSEC, and physical security.



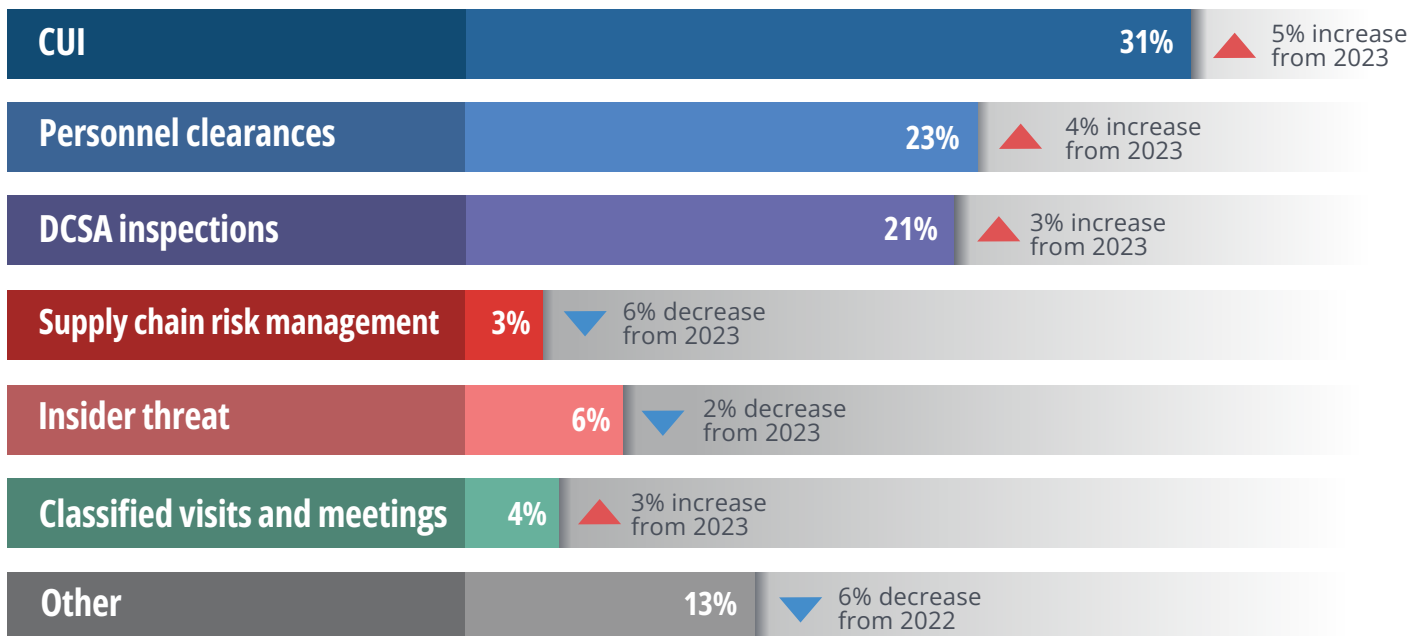
WHAT IS YOUR BIGGEST PAIN POINT IN THE SECURITY CLEARANCE PROCESS?



With clearance processing times ticking back up it's not surprising that slow security clearance processing times were the biggest pain point in the clearance process, more than double the next most likely response. Most other issues, including reciprocity and DISS, hovered close to the prior year's responses. Responses in the 'other' category included issues obtaining polygraph appointments and the NBIS transition/working with different IT systems.

Personnel vetting is cumbersome, but it's not the only task security officers face. Navigating the world of Controlled Unclassified Information (CUI) continues to be a top pain point for FSOs, with even more reporting it as their number one source of grief. Responses in the 'other' category included 'constantly changing government requirements' and 'government not following the NISPOM.'

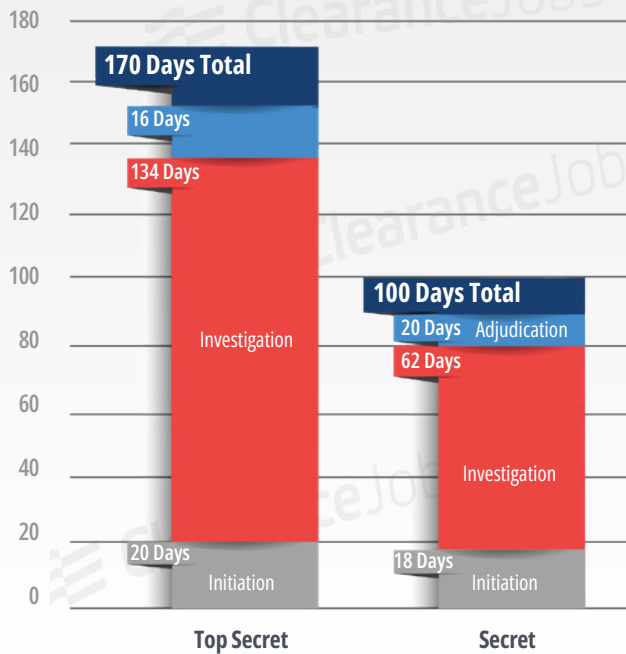
WHAT ASPECT OF YOUR JOB CREATES THE MOST HEADACHES?



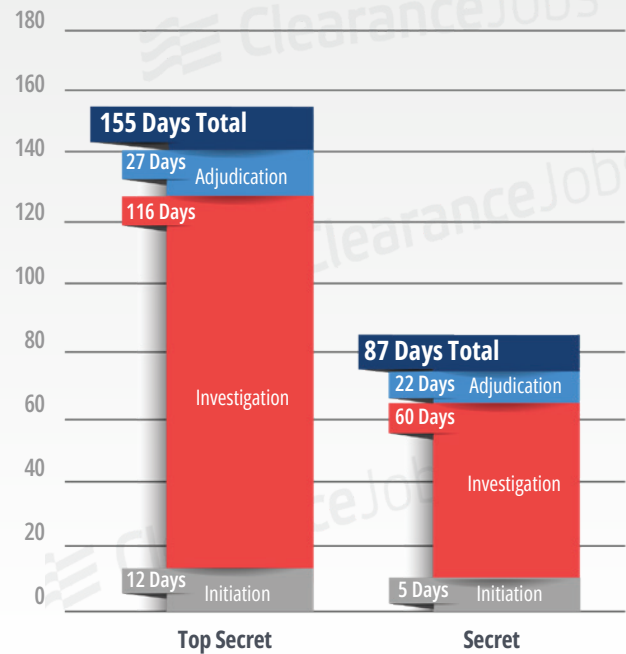
AVERAGE CLEARANCE PROCESSING TIMES

Security clearance processing times remain the number one pain point in the clearance process. Security clearance processing times continue increasing, which means this may remain a painpoint for security officers looking to quickly onboard personnel and dealing with the ongoing questions from candidates wondering about their status.

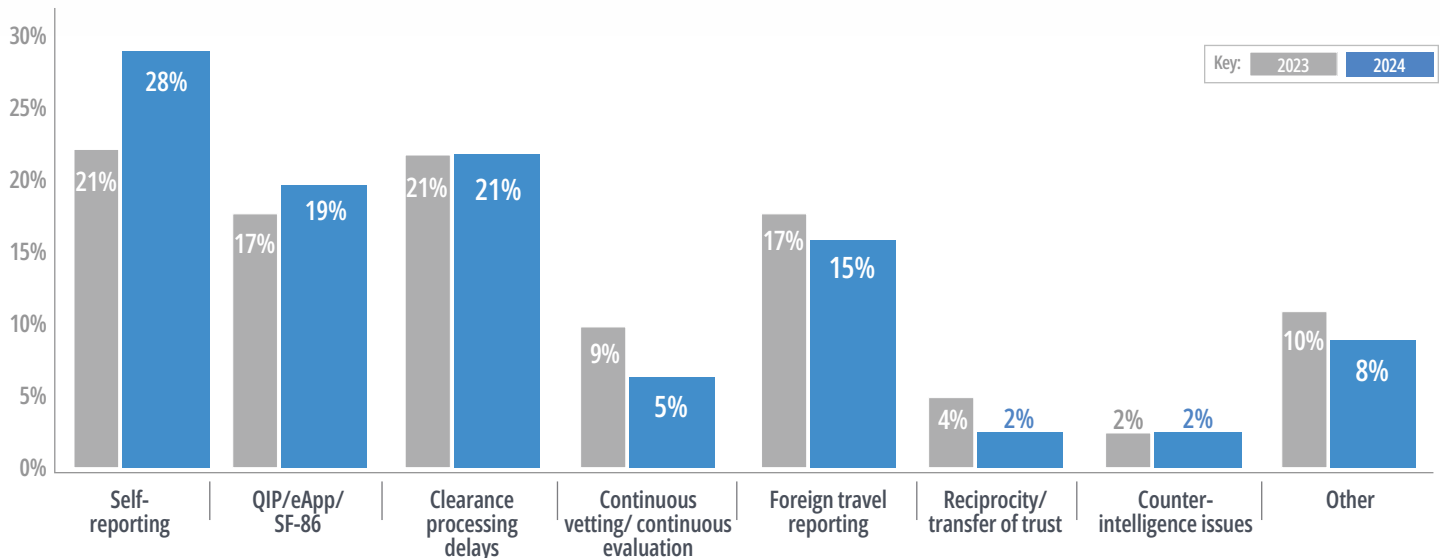
HOW LONG IT TAKES TO OBTAIN A DOD/INDUSTRY SECURITY CLEARANCE



HOW LONG IT TAKES TO OBTAIN A GOVERNMENT-WIDE SECURITY CLEARANCE

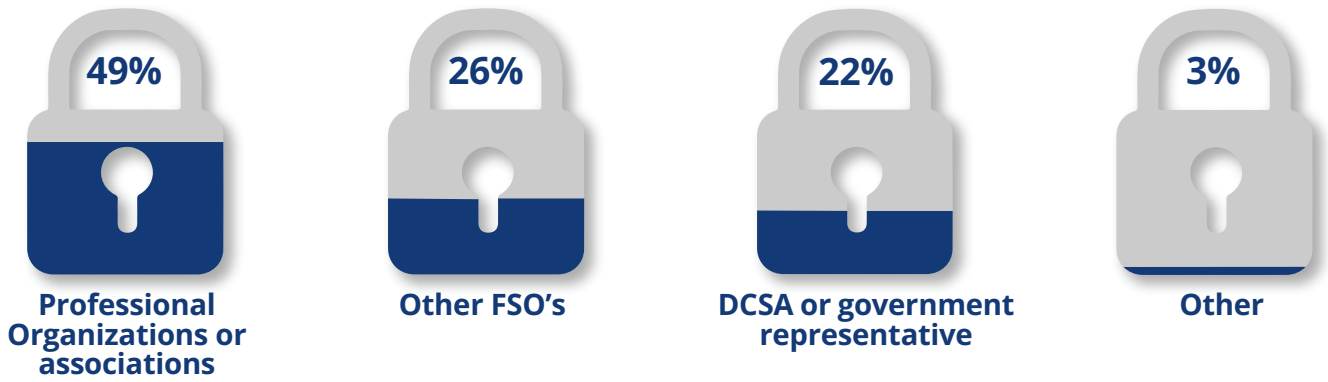


WHAT TOPIC GENERATES THE MOST QUESTIONS FROM EMPLOYEES OR APPLICANTS?



Self-reporting is still the most-asked question from clearance applicants. The good news is Continuous Vetting (CV) and reciprocity questions went down. As reciprocity figures continue to improve, with reciprocity into the DoD now taking an average of a day, it's hopeful fewer candidates will struggle with questions as they look to transfer their clearance eligibility. And while CV continues to create some policy issues and discrepancies for FSOs looking for guidance, it's clear applicants have made a seamless transition into the system.

WHEN YOU HAVE QUESTIONS, WHERE DO YOU GO FOR THE BEST GUIDANCE?

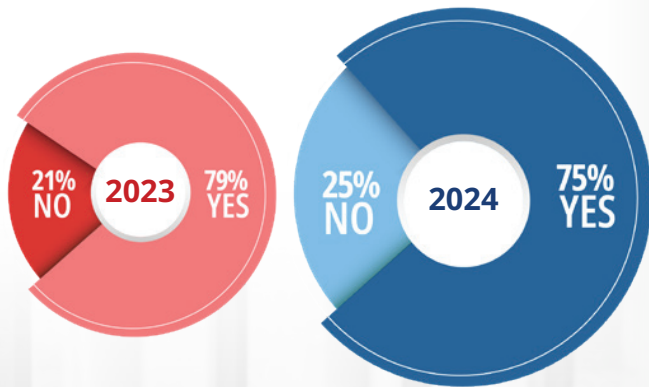


Professional organizations continue to dominate as the key source of information and advice for security officers. They're considered so vital, 97% of respondents reported belonging to at least one. DCSA or government representatives continue to go down as a key source of information, pointing to the ongoing need for better translation of government policy to actual process for FSOs.

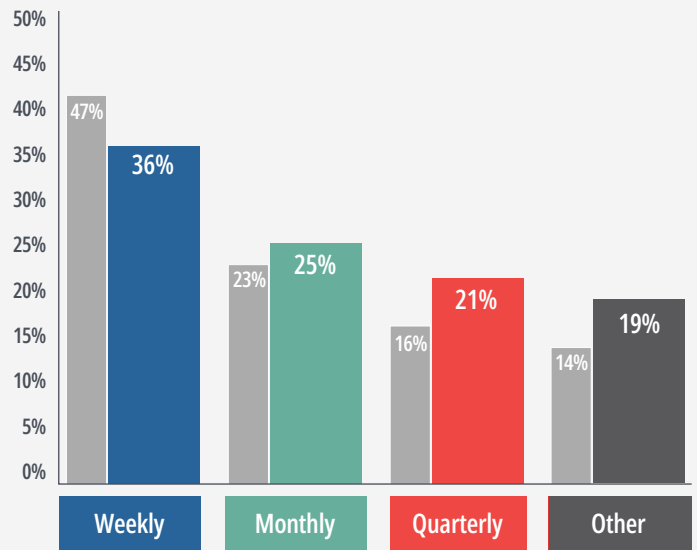
DO YOU BELONG TO ANY SECURITY PROFESSIONAL ORGANIZATIONS?



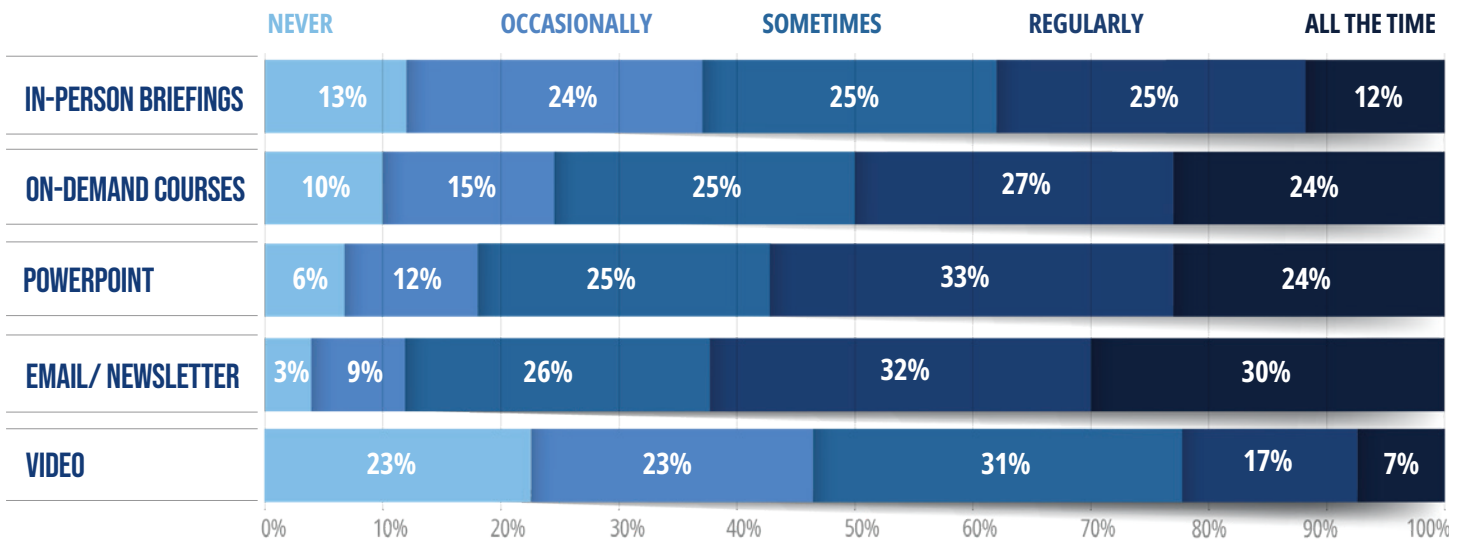
DO YOU REGULARLY BRIEF OR MEET WITH LEADERSHIP/C-SUITE EXECUTIVES?



HOW OFTEN DO YOU REGULARLY BRIEF OR MEET WITH LEADERSHIP?

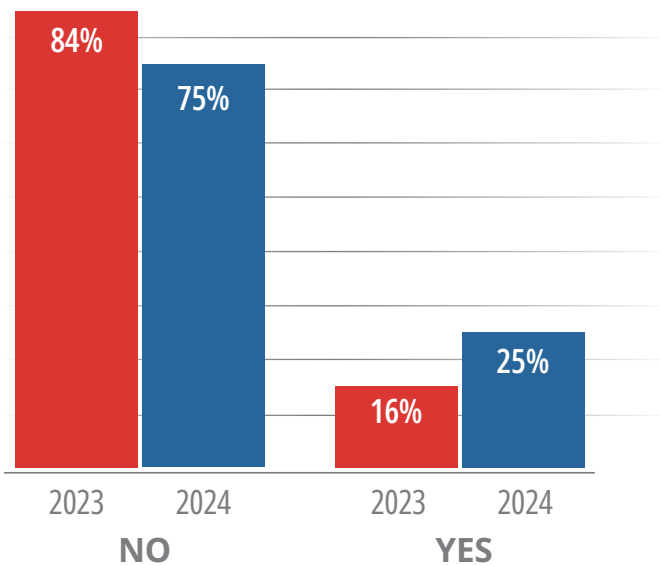


HOW OFTEN DO YOU USE EACH OF THESE TRAINING METHODS?

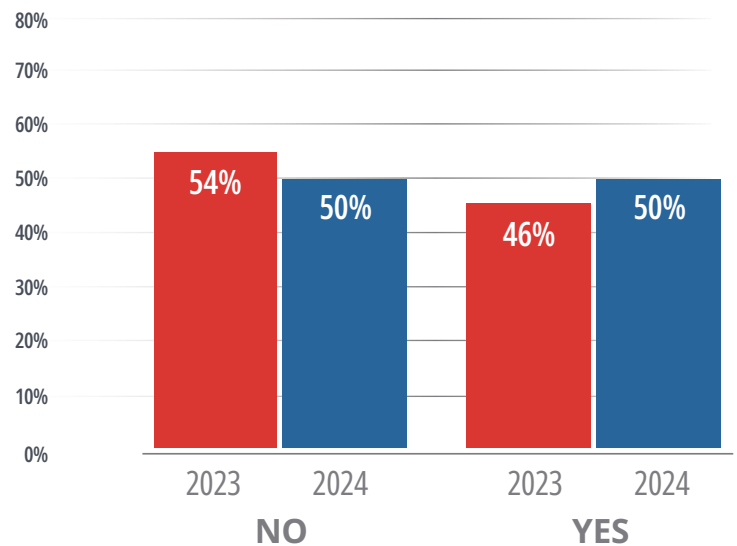


PowerPoint, email, or newsletters remain the prominent training method used by security professionals. In a sign of office return-to-work policies, more respondents also note at least sometimes using in-person briefings. And while video is the online media platform experiencing a meteoric rise in use and viewership, for security officers, it's more like a fizzle, with use of video for training platforms staying largely stagnant over the past three years.

DO YOU USE THIRD-PARTY VENDORS TO ASSIST WITH SECURITY TRAININGS?

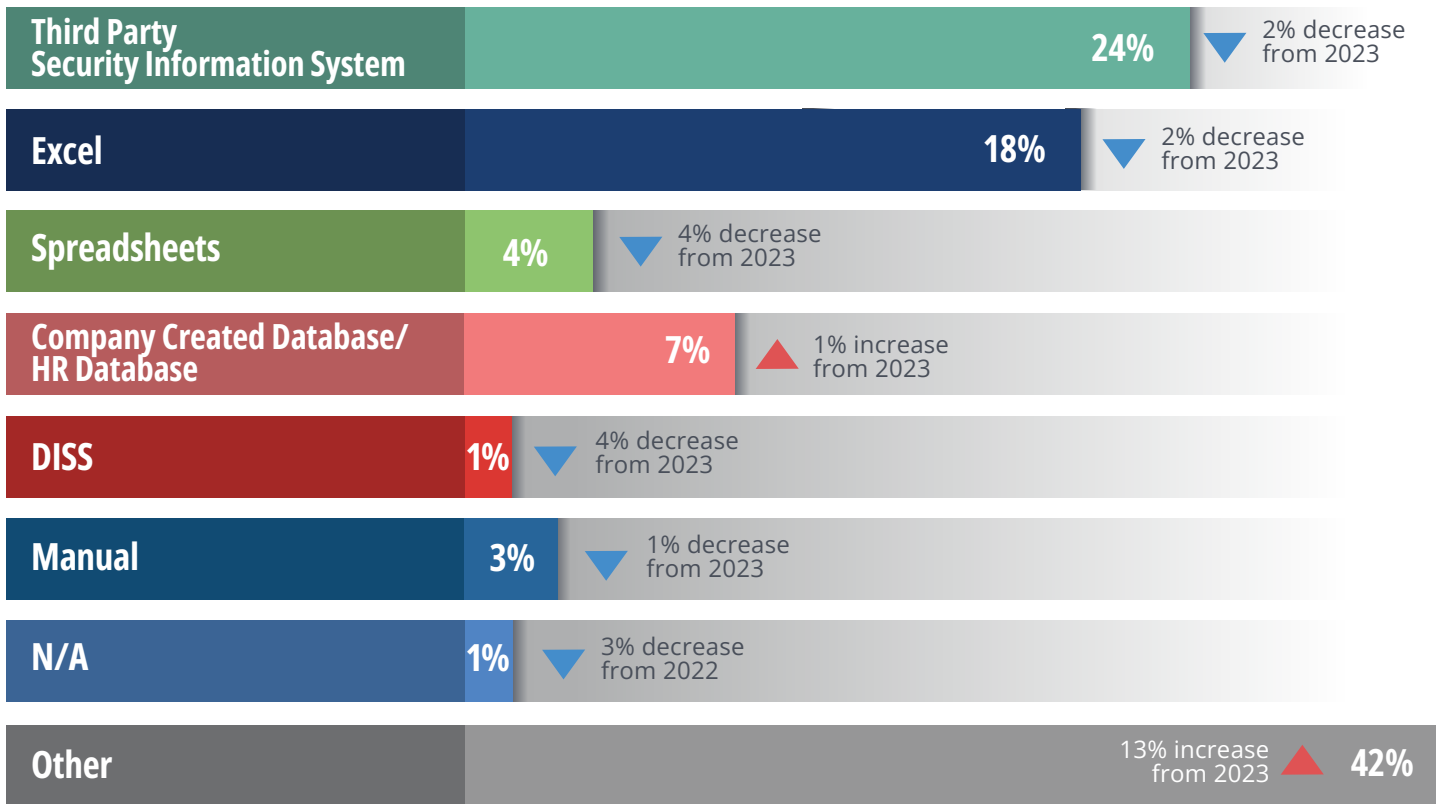


DO YOU USE A SECURITY INFORMATION MANAGEMENT SYSTEM?



While lack of resources is still cited as a significant issue preventing FSOs from having the tools necessary to do their jobs, the good news is that more are reporting getting help with training. Fortunately, unlike last year, no respondents reported using a paper-based system to keep track of cleared personnel, but the majority still note that Excel or internal spreadsheets are the method in use.

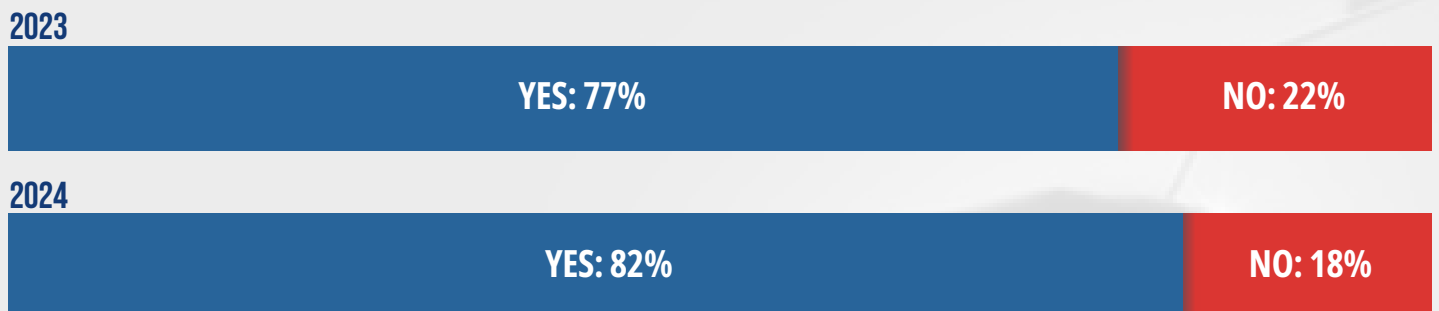
WHAT SOFTWARE DO YOU USE/HOW DO YOU TRACK YOUR INFORMATION?



“The complexity of the role security officers play in their organizations is only increasing,” said Michael Struttman, CEO of SIMS Software.

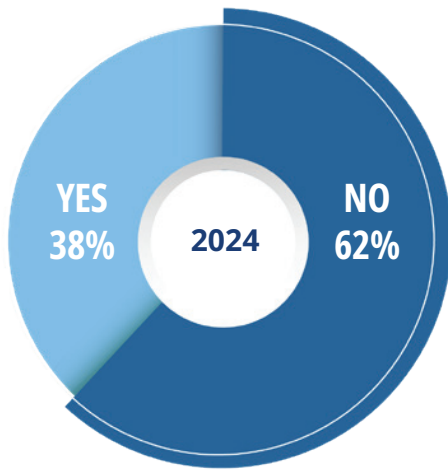
“Topics from CUI to self-reporting and SEAD-3 are generating a lot of questions from the workforce and increasing the workload for security officers. This is where Senior Management Officials can step in to provide the resources, accountability and support to ensure both their programs and bottom lines are safeguarded from the rising tide of threats.”

DO YOU FEEL YOU CURRENTLY HAVE THE TECHNOLOGY NECESSARY TO DO YOUR JOB WELL?



Slightly more respondents noted having the technology necessary to do their jobs, a figure that still falls behind the percentage from 2022. When asked what prevented them from having the technology necessary to do their jobs, the majority noted budget or lack of leadership buy-in. And in a telling response from one Assistant FSO, the response was, ‘the FSO.’

DO YOU HAVE DIFFERENT SECURITY REQUIREMENTS FROM YOUR CUSTOMER?



New this year, we asked respondents if they had differing security requirements from their customers, and 38% of respondents noted they did. When it came to what those differences were, the responses were vast, from different policies around SCI, to adverse information reporting, onboarding processes and forms and complaints of customers running collateral programs with SAP policies. Many noted the differences between DoD and IC policies, but others said contracts even within the same government agency could operate with completely different security policies. One respondent summed it up well, noting it “Spans a large swath, from nothing to everything.”

The state of the security officer today shows security officers trying to stay afloat despite a stream of new policies, IT systems, and differing customer requirements. CMMC, CUI, and staying abreast of all the changes remains an incredibly challenging job. And while the experience of the workforce – 73% report 10 or more years of experience – is a positive, the lack of entry-level talent is denying the industry the energy and innovation that help to fuel growth and keep pace with change. Professional organizations are clearly not just optional, but a vital part of keeping security officers informed and engaged, and the good news is security officers are clearly taking advantage. The FSO plays a critical role in protecting national security, and ensuring security programs have the information and resources they need to succeed is a critical national security function.

The advertisement features a dark blue background with a pattern of glowing, wavy lines. The text is white and light blue. The SIMS INFINITY logo is in the top right corner. The main headline is 'The Next Generation SIMS'. Below it is the tagline 'The Leading Security Information Management System'. A list of six features is presented in two columns, each with a small icon. At the bottom left is the SIMS SOFTWARE logo, and at the bottom right is the website URL SIMSsoftware.com.

The Next Generation SIMS

The Leading Security Information Management System

- Modern Web-based User Interface
- Powerful & Highly Customizable
- Systemwide Enhancements & Upgraded Features
- High Speed Performance
- Extensive Role-based Permissions
- New Hub Communications & Actions Center

SIMS[®]
SOFTWARE

SIMSsoftware.com