ClearanceJobs®

40 YRS SIMS® SOFTWARE

CLEARANCEJOBS STATE OF THE FACILITY SECURITY OFFICER 2023

CLEARANCEJOBS IS THE LARGEST CAREER NETWORK FOR PROFESSIONALS WITH FEDERAL GOVERNMENT SECURITY CLEARANCE.

STATE OF THE FACILITY SECURITY OFFICER

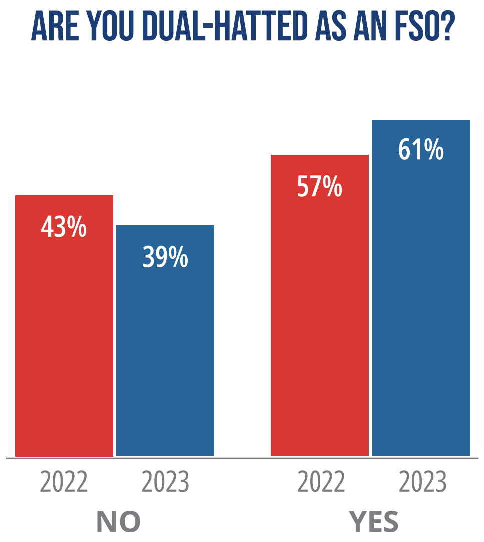
Behind every security clearance or classified program is a security officer maintaining that eligibility and keeping those classified programs safe. The good news is security clearance reforms baked into Trusted Workforce 2.0 are beginning to move the needle in the right direction when it comes to common issues like reciprocity and clearance processing times. The bad news? New initiatives like Controlled Unclassified Information (CUI) are coming fast and hot on the heels of security officers today.

Perhaps the biggest issue affecting the security workforce today is the one facing the overall national security community – an increasingly gray workforce. The good news is an enviable 72% of security professionals cited more than 10 years of experience. The bad news? There are fewer professionals today than in last year's report citing 6 years or less of experience, which could signal fewer young professionals entering the profession.

Perhaps the worst issue facing security professionals today is the lack of those taking advantage of software and resources to assist them in their training and security clearance tracking efforts. While more security officers report being in weekly contact with the C-suite, perhaps too few are taking advantage of the opportunity to advocate for more funds and resources to help them accomplish the mission. Or if they are, those requests are not leading to a greater allocation of dollars.

Most concerning of all is the fact that 2% of respondents said they were using a paper-based system to keep track of their cleared personnel. When failure to keep clearances up-to-date could end in contract loss or criminal prosecution, relying on a paper system isn't just a security risk, it's a business risk, as well.

A growing number of respondents were dual-hatted into another role beyond FSO, 62%. When they're not maintaining classified programs, security officers are also working in HR roles, recruiting, cybersecurity, and information assurance.


ARE YOU DUAL-HATTED AS AN FSO?

7% fall into HR and recruiting roles

● Equal to 2022

6% double as cybersecurity specialist

▲ 1% increase from 2022

6% also act in information assurance

▲ 2% increase from 2022

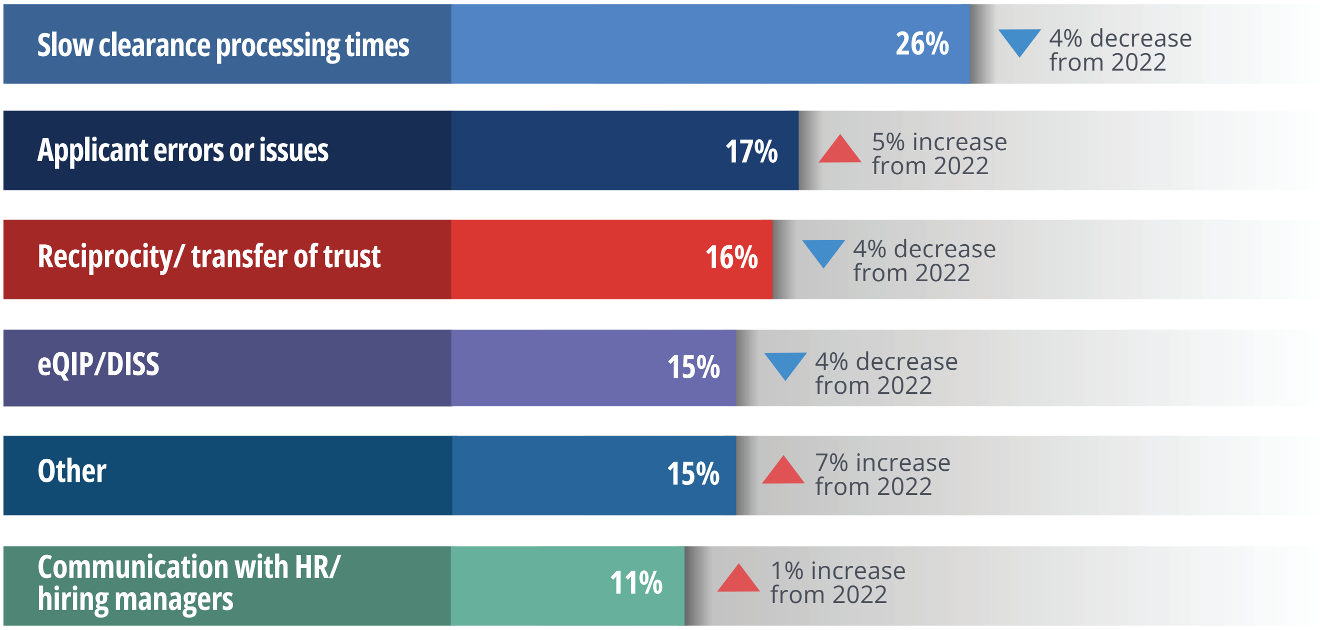
4% spend time in business development

▼ 1% decrease from 2022

39% serve in another role, from contract manager or office manager to technical writer or finance manager.

▲ 1% increase from 2022

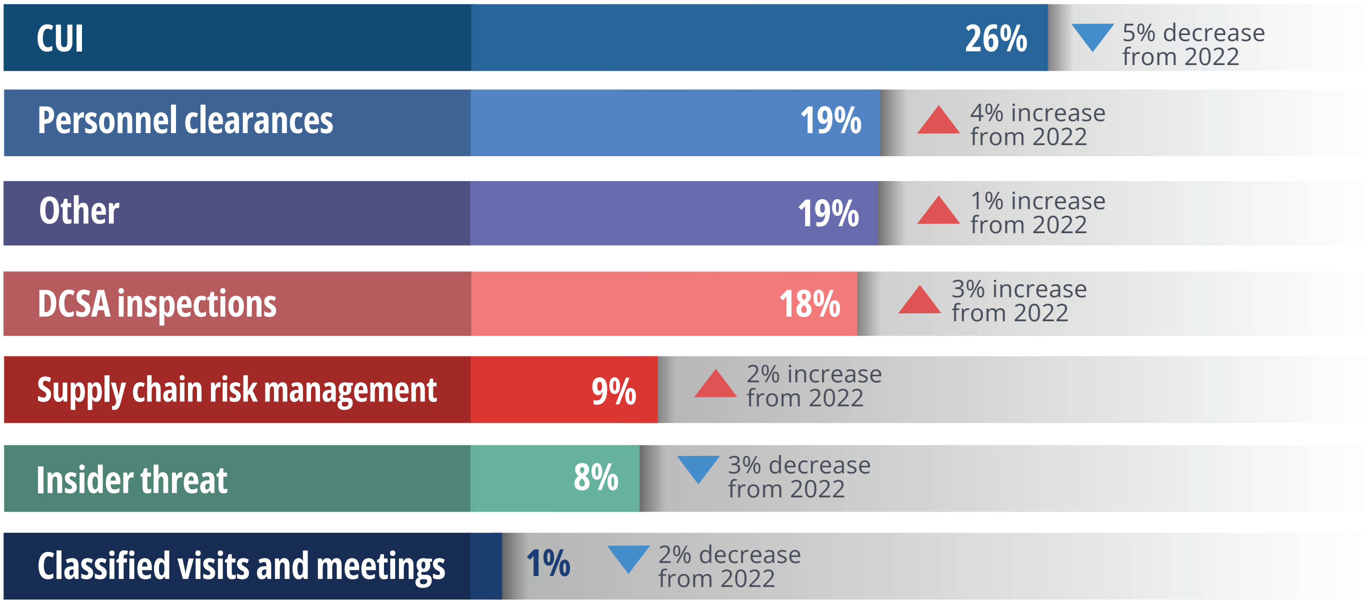
WHAT IS YOUR BIGGEST PAIN POINT IN THE SECURITY CLEARANCE PROCESS?



The good news is the usual suspects when it comes to pain points are down in almost every area (other than applicant errors/issues). DISS transfer issues appear to have been somewhat addressed, with fewer respondents citing eQIP and DISS as pain points. For the 15% of respondents who cited 'other' as their key pain point in the clearance process, the responses ranged from inconsistencies with government customers, CAC credentialing, or everyone's favorite four letter acronym – NBIS, the National Background Investigation Services.

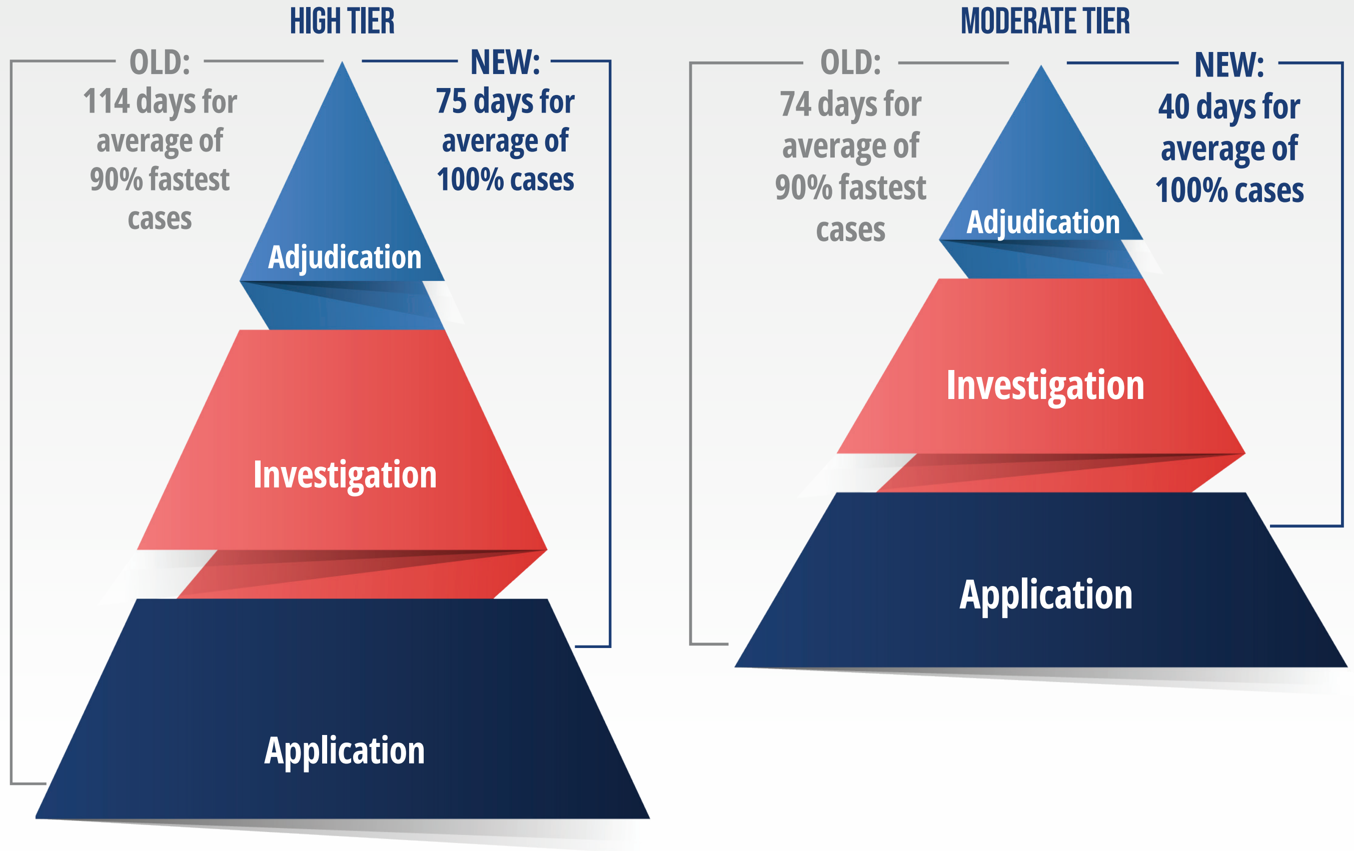
When it comes to the broader job and not just the clearance process, CUI continues to dominate as a pain point, although the percentage has dropped slightly. Headaches coming up in the 'other' category including not being included in the proposal process, training, and the process for assigning and tracking data.

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. That number is going down, along with average clearance processing times. And thanks to new, even more aggressive benchmarks announced in March, security officers should expect vetting timelines to continue decreasing.



HIGH TIER

OLD: 114 days for average of 90% fastest cases

NEW: 75 days for average of 100% cases

Adjudication

Investigation

Application

MODERATE TIER

OLD: 74 days for average of 90% fastest cases

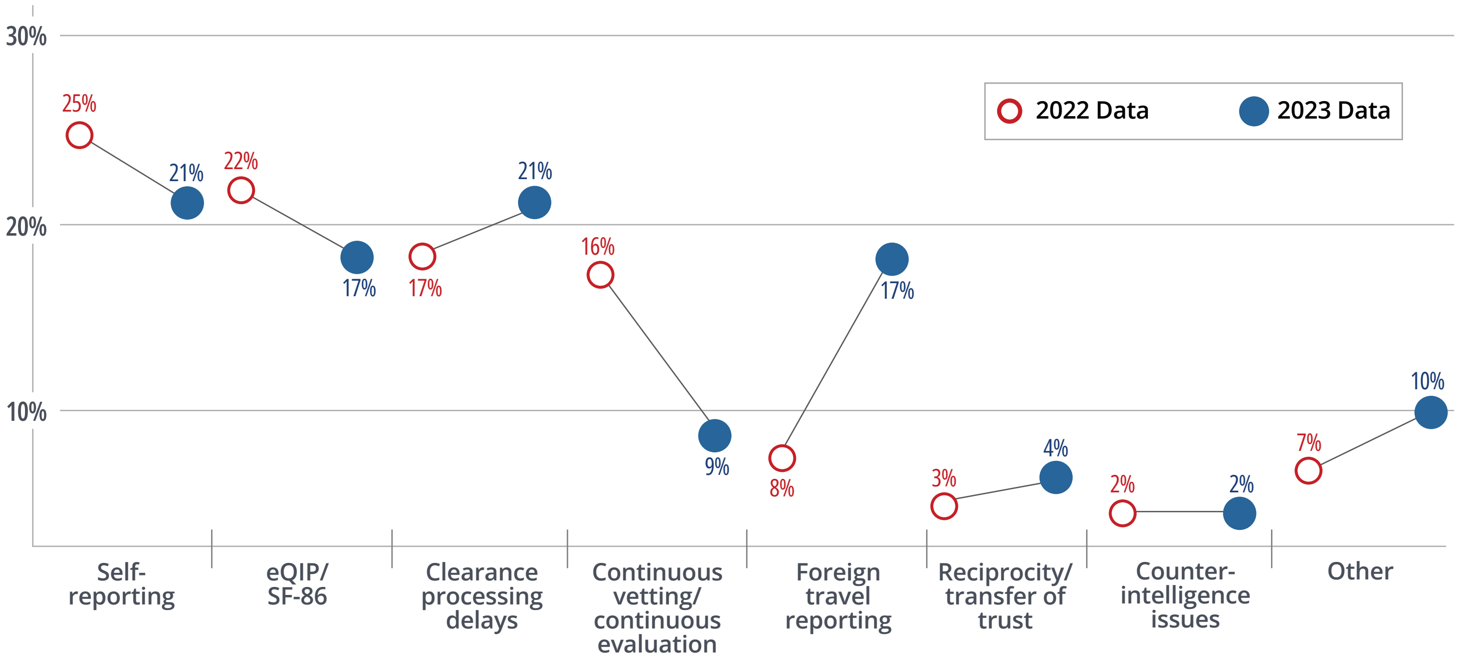
NEW: 40 days for average of 100% cases

Adjudication

Investigation

Application

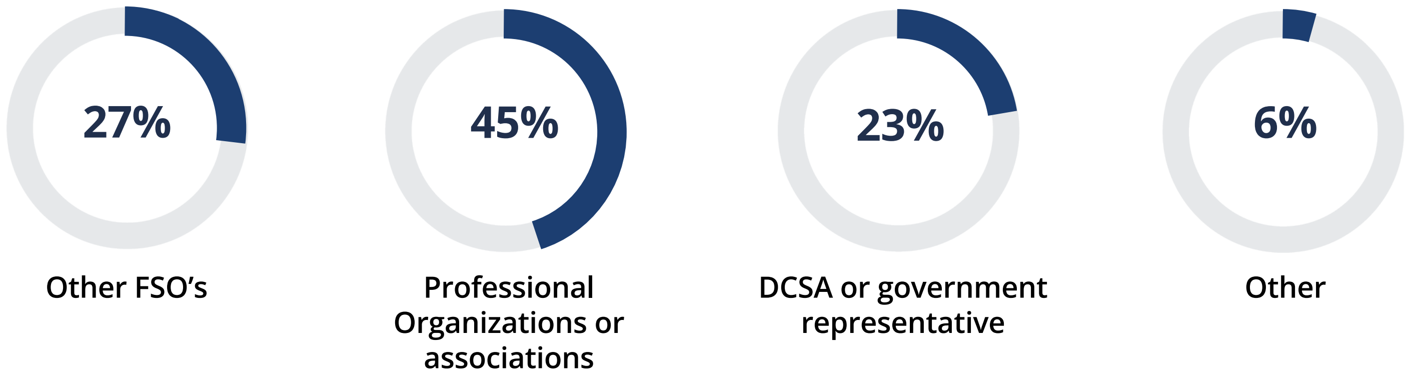
WHAT TOPIC GENERATES THE MOST QUESTIONS FROM EMPLOYEES OR APPLICANTS?



Questions about SF-86 issues are down, but concerns about reporting foreign travel are up. New foreign travel reporting requirements under Security Executive Agent Directive (SEAD) 3 have been supported within DISS for less than a year now, and many employees or applicants still wonder what is required.

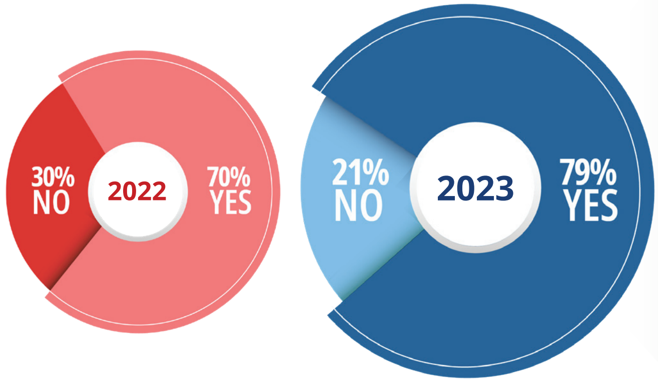
When it comes to issues in the 'other' category, it's not just FSOs having issues with CUI –top areas for candidate questions in the 'other' category were CUI and another 'c' word – cannabis.

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

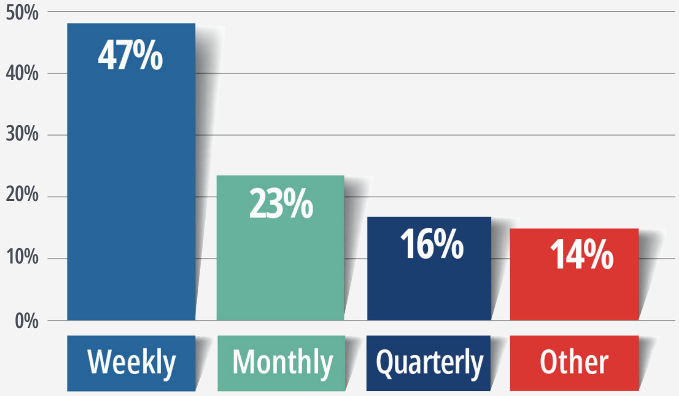


Professional organizations saw a major uptick in positive responses in 2023, with 45% of respondents saying professional organizations and associations were their go-to source for the best guidance. Those citing a DCSA or government rep were down. DCSA established a new field structure in 2021, but the agency is continuing to work to address any issues arising from the consolidation of Defense Security Service mission and the consolidation of personnel and industrial security under one umbrella.

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

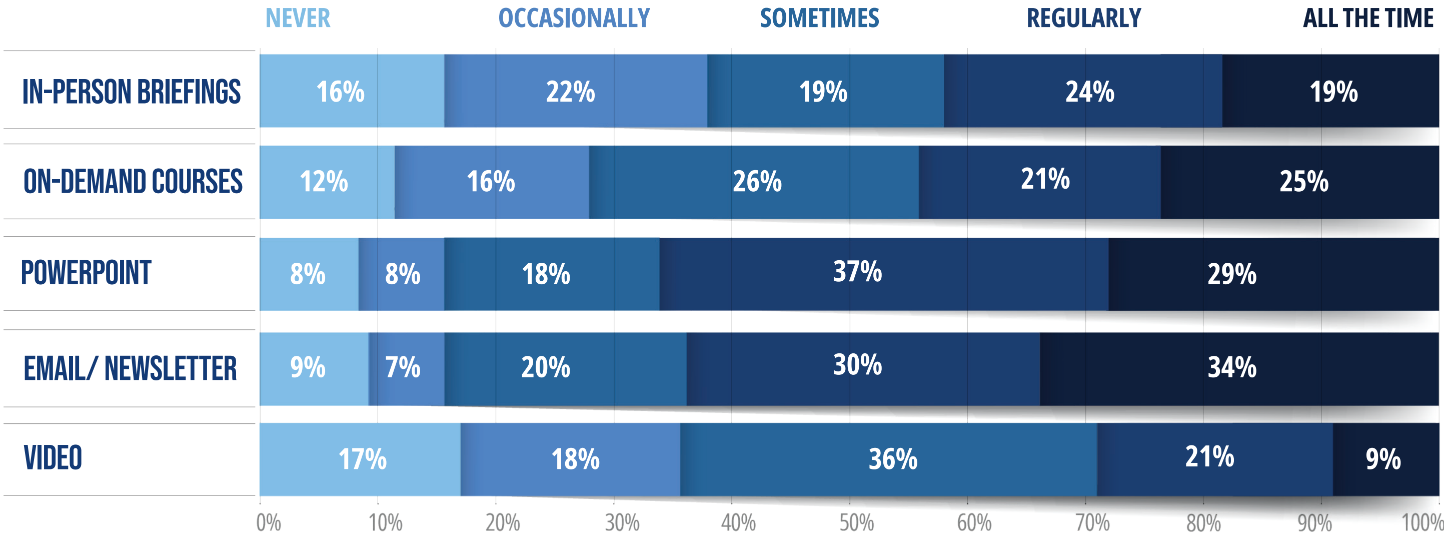


HOW OFTEN DO YOU REGULARLY BRIEF OR MEET WITH LEADERSHIP?



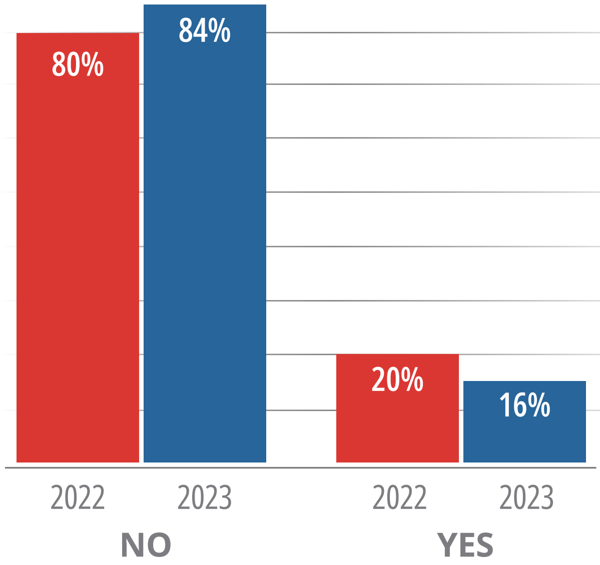
The importance of security is often evidenced by how much the C-suite is engaged in security activities. The good news is 79% of security officers regularly meet with their leadership. The bad news is, 21% don't. The number of respondents meeting with leadership weekly has gone up, and that's also good news.

HOW OFTEN DO YOU USE EACH OF THESE TRAINING METHODS?

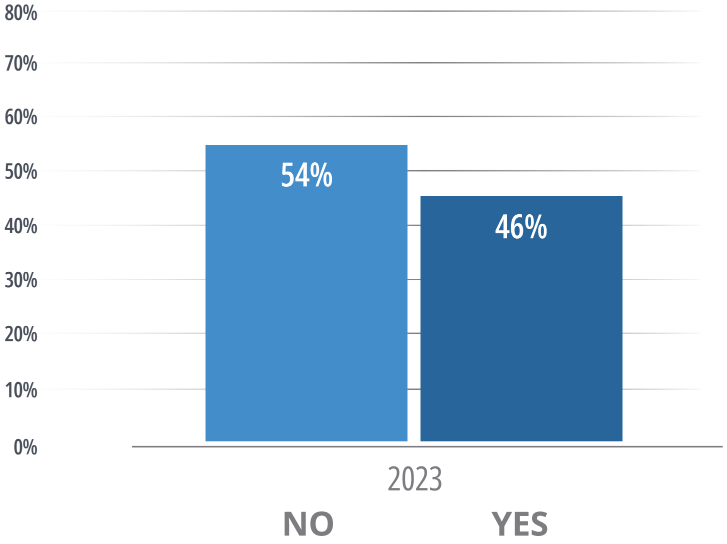


PowerPoint and email or newsletters remain the prominent training method used by security professionals, but on-demand courses, webinars, and video had a year-over-year uptick. While there are fewer respondents who note they never use video, it's clearly the lesser used training method. While there are fewer respondents who note they never use video, it's clearly the lesser used training method.

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



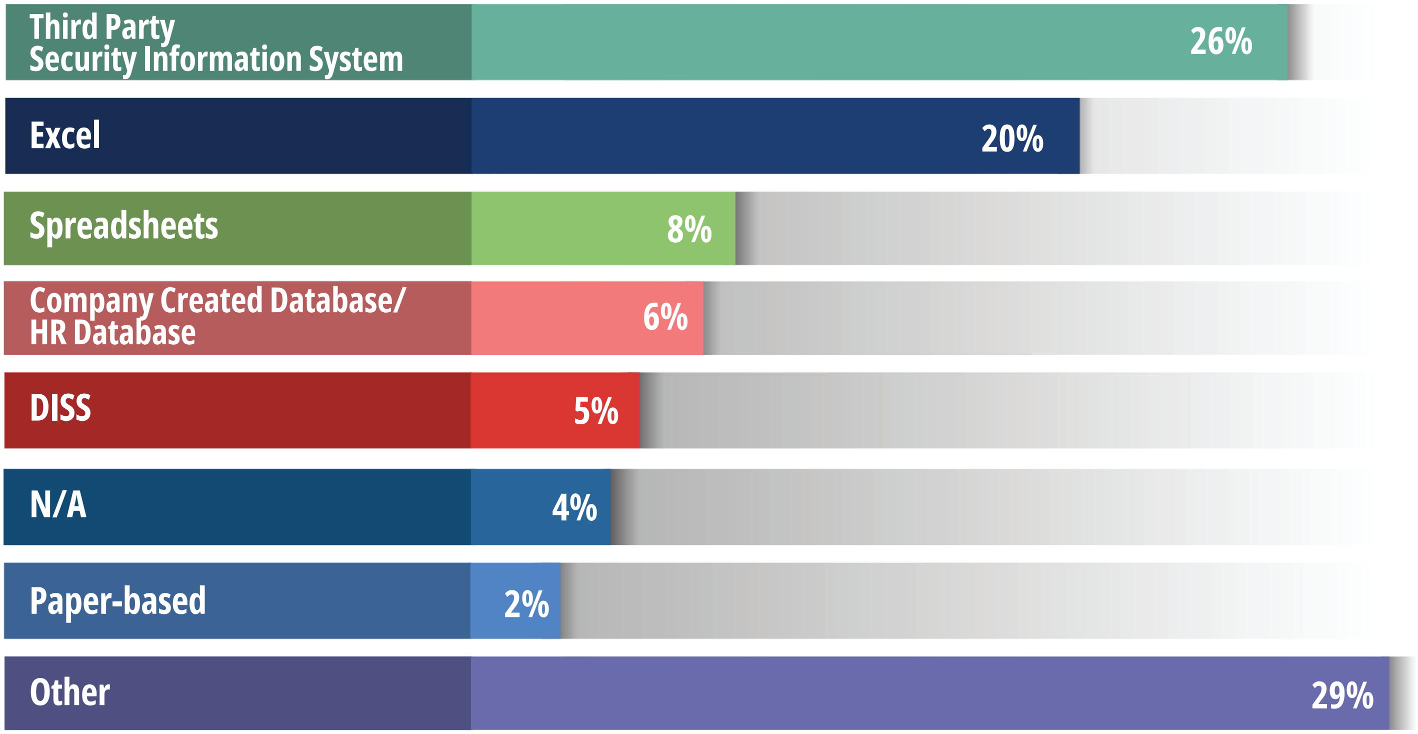
DO YOU USE A SECURITY INFORMATION MANAGEMENT SYSTEM?



Security professionals aren't getting any younger – and they aren't getting any more help when it comes to security training and management systems. Just 16% use third parties to assist with security trainings, and less than half (46%) use a security information management system.

In the wake of a recent news report that lapsed security clearances were an issue for more than 250 personnel involved in the Air Force One program, it's a clear reminder that keeping track of personnel security records is a vital aspect of any security office.

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

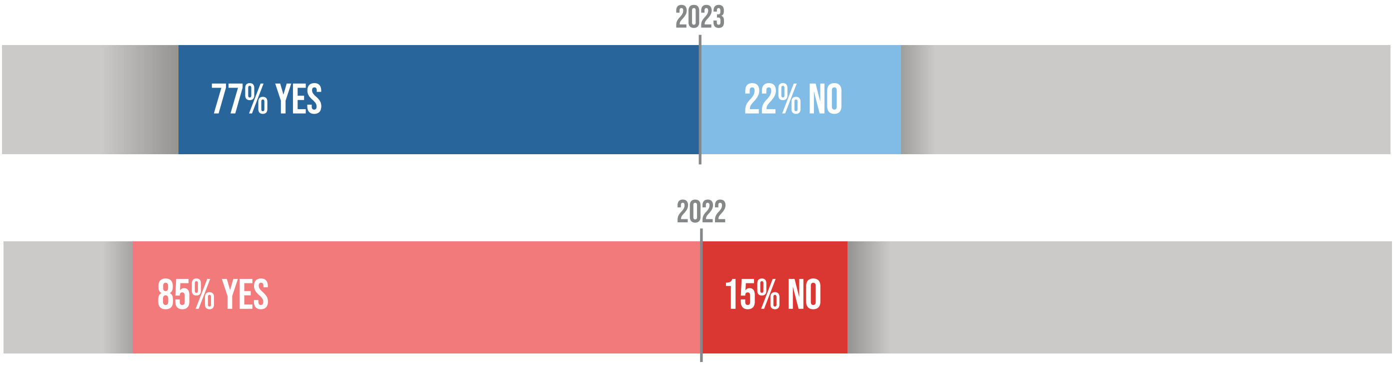


When asked how they are keeping track of their information, what may be most shocking is that 2% admitted to using a paper-based system to track their cleared personnel. Among those citing ‘other’ as the response, there were a variety of methods from desktop files to ‘the cybersecurity team does it.’

“Security officers have a vital national security function, “said Michael Struttmann, CEO of SIMS Software. “I think this is a clear area where security professionals need support, and where companies and their accountable Senior Management Officials can step up and provide the resourcing to ensure not just the security of programs, but the stability of their business in this critical compliance area.”

As Trusted Workforce 2.0 continues to roll out, there will be even more professionals within the government’s Continuous Vetting (CV) program, and more opportunities, for personnel to transfer between contracts. That’s good news for business – but bad news for security where paper-based systems and spreadsheets reign supreme.

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



In what is a clear sign that security officers are feeling the strain of tracking their personnel, there was an 8% uptick in the number of respondents who said they don't have the technology necessary to do their jobs well. When asked for more specifics, they cited a lack of investment in technology and manual tracking of employees as pain points in the process.

Security professionals today are under increasing pressure – improvements in the personnel security process also means changes for security officers to embrace. Whether it's DISS or NBIS, CV or reciprocity – new challenges (and acronyms, and systems), just keep coming. While it's clear the C-suite is starting to take personnel vetting and facility security seriously, as evidenced by the number of respondents meeting weekly with their leadership, if those meetings aren't also leading to resources for security to perform the job, a critical gap remains.

The other gap is in the number of respondents at the entry-level. While experience is key, so is having enough new personnel to fill roles as more experienced professionals retire. As the complexity and breadth of the personnel security program continues to grow, it needs the tools, resources, and staffing to address it.

40 YRS SIMS® SOFTWARE
SIMSsoftware.com
Infinite data. Infinite risk mitigation.
One infinite solution.
Tracked
Track your vital information, safely and securely.
Consolidated
Make efficient decisions driven by data.
Integrated
Gain a 360° view of every asset.