How Employers Can Mitigate Insider Threats

Employment and Labor

CHEAT SHEET

- ***Ban the Box.*** A growing number of US states have passed “Ban the Box” legislation that prohibits an employer’s request for arrest or conviction records on initial job applications.
- ***UK considerations.*** In the United Kingdom, employers can’t reject an applicant for a job because they’ve been convicted of an offense after its “spent” period — which is a term used to refer to a designated rehabilitation period set forth by the UK Rehabilitation of Offenders Act of 1974.
- ***Follow the EEOC.*** The Equal Employment Opportunity Commission released enforcement guidance restricting the use of arrest and conviction records in hiring practices. In-house counsel should be mindful of these regulations to ensure compliance.
- ***Integrate and communicate.*** By integrating security officials, HR, and the legal department into hiring decisions, companies can mitigate the risk of insider threats while remaining in compliance.

For any company, its employees are one of its most valuable assets. But ensuring that you are hiring the right people — people who share your company culture and values — is not straightforward. When things go sideways, you wonder: “What did we miss?” Security experts argue that thorough background reviews are the key to preventing hiring the wrong people, but seasoned human resources (HR) professionals caution against using certain information discovered in a background check. This article examines both the legal and practical perspectives that can help you, and your company, make the best decision to protect your business and workforce.

What can I do?

Employers often regard applicants with criminal records as higher risk, due to concerns about perceived and/or potential dependability, conduct problems, or trustworthiness issues. When developing selection criteria, many employers have increased their vigilance by developing early detection processes, typically at the application stage, to identify or weed out these candidates. However, as employers have widened the scope of their screening processes, more and more candidates are caught in the pool of potentially unemployable candidates. This has resulted in a societal pushback aimed precisely at removing barriers to employment for this group.

For example, a growing number of US states have passed so-called “Ban the Box” legislation that prohibits or restricts an employer’s request for arrest or conviction records on initial job applications. Other legislation has focused on precluding how many years for such records an employer may consider in making employment decisions. Former US President Barack Obama specifically noted the barriers for employment that are posed by an employer’s use of arrest or conviction records. He called upon agencies within the federal government to take steps to curtail their use. In response, the US Equal Employment Opportunity Commission (EEOC) in 2012 issued its highly anticipated enforcement guidance (EEOC guidance) regarding the use of arrest and conviction records, and compliance with Title VII of the US Civil Rights Act of 1964. That guidance explicitly focused on the disproportionate impact that the use of arrest and conviction records has on minority applicants. In 2014, the EEOC and the US Federal Trade Commission FTC) issued a joint publication on employment-based background checks and compliance with federal laws. This publication more broadly focused on the use of incomplete and inaccurate information, and the legal requirement that applicants and employees must be notified of their rights to review and contest the information if and when it becomes an impediment to employment.

While both state and federal authorities view the use of prior arrest and conviction information with hostility, there is still recognition of the legitimate use of the information, particularly in security-related positions, including those in which the employee holds the ability to handle or possess classified information. Most significant to the security industry, particularly those who deal with classified information, the publications and regulations clarify that it is not unlawful for employers to obtain or use arrest or conviction records. Rather, the EEOC seeks to ensure such information is not used in a discriminatory way, or in a way that violates other applicable laws. Moreover, when conducting background checks through a company in the business of compiling background information, an employer must comply with the US Federal Credit Reporting Act (FCRA) — a law that imposes time restrictions on background information.

Many gray areas concerning background checks remain despite — or because of — EEOC and FTC guidance. The issues are further complicated by the unique circumstances inherent in screening and hiring individuals for positions of national security. Additionally, companies may struggle to implement

the appropriate procedures because not all of the employees hold a security clearance. Information regarding arrests and convictions, including the date they occurred, is critical when determining whether certain “Adjudicative Guidelines for Determining Eligibility for Access to Classified Information,” as the US government puts it, will be raised. If this happens, it would affect an applicant’s ability to successfully obtain and maintain the security clearance necessary for the position in question.

At a minimum, lawyers and security and HR professionals who work at companies with facility clearances (FCLs)* should be mindful of these laws and regulations. The US government now requires that all entities with a facility clearance under the National Industrial Security Program (NISP) establish an Insider Threat Program to identify employees who may be bad actors. The lack of communication between HR and security can cause more than just friction between functional areas. Rather, the failure to communicate can result in employer liability issues such as defamation claims, negligence in filing reports, and intentional infliction of emotional distress.

* An FCL is an administrative determination by the US Government that an entity is eligible for access to classified information or award of a classified contract. See Department of Defense Manual 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) at §2-100.

The EEOC generally discourages inquiries into arrests and convictions

The EEOC distinguishes between arrest and conviction records. The EEOC guidance makes it clear that it believes the use of arrest records in employment decisions is neither job-related nor consistent with business necessity. Because minority candidates are disproportionately arrested, the use of an arrest record would have a disproportionate effect on minorities and, therefore, would not comply with Title VII prohibitions against discrimination. Moreover, the EEOC reasons that an arrest, unlike a conviction, does not establish (1) that criminal conduct has actually occurred, (2) that the person in question was actually responsible for the unlawful conduct, or (3) the final outcome of the arrest. That is not to say that the fact of the arrest cannot be used at all. Consistent with the overarching theme of the EEOC guidance, an employer may question the applicant concerning an arrest and consider the underlying conduct referenced in the arrest report if the conduct makes the individual unfit for the position at issue.

A less restrictive approach is taken regarding convictions. The EEOC advises employers to reconsider their present applications and remove blanket, “catch-all” questions that ask whether the individual has been convicted of any crimes. However, if and when an employer chooses to make inquiries on this topic, the employer should be able to demonstrate the criminal background information is (1) job related and (2) consistent with business necessity. Employers are advised to judge each situation on its own merits, and conduct and document an ad hoc determination of this analysis.

An employer can successfully use the “job-related and consistent with business necessity defense” if, in screening applicants for criminal conduct, it (1) considers at least the nature of the crime, the time elapsed since the criminal conduct occurred, and the nature of the specific job in question, and (2) gives an applicant who is excluded by the screen the opportunity to show why he or she should not be excluded (also referred to as an “individualized assessment”). Regarding the time elapsed since the criminal conduct, the EEOC generally considers convictions older than seven years to be unrelated to employment worthiness. The EEOC bases this limit on its reading of sociological studies

that suggest a person with an old conviction has no greater likelihood of engaging in unlawful conduct than a person without a criminal conviction.

In an effort to provide practical implementation tips, the guidance includes a “Best Practices” list for employers’ consideration {see sidebar}. These “Best Practices” do not have the force of law, but give some insight into the EEOC’s expectations.

EEOC “Best Practices”

GENERAL

- Eliminate policies or practices that exclude people from employment based on any criminal record.
- Train managers, hiring officials, and decision makers about Title VII and its prohibition on employment discrimination.

DEVELOPING A POLICY

- Develop a narrowly tailored written policy and procedure for screening applicants and employees for criminal conduct.
    - Identify essential job requirements and the actual circumstances under which the jobs are performed.
    - Determine the specific offenses that may demonstrate unfitness for performing such jobs.
- Identify the criminal offenses based on all of the available evidence.
    - Determine the duration of exclusions for criminal conduct based on all available evidence.
    - Include an individualized assessment.
    - Record the justification for the policy and procedures.
    - Note and keep a record of consultations and research considered in crafting the policy and procedures.
- Train managers, hiring officials, and decision makers on how to implement the policy and procedures consistent with Title VII.

QUESTIONS ABOUT CRIMINAL RECORDS

- When asking questions about criminal records, limit inquiries to records for which exclusion would be job related for the position in question and consistent with business necessity.

CONFIDENTIALITY

- Keep information about applicants’ and employees’ criminal records confidential. Only use it for the purpose for which it was intended.

Source: www.eeoc.gov/laws/guidance/arrest_conviction.cfm

The EEOC retains some employer protections for positions of national security

The EEOC acknowledges that some industries are subject to federal statutory and/or regulatory requirements that prohibit individuals with certain criminal records from obtaining or holding particular positions. By way of example, the EEOC notes that “federal law excludes an individual who was convicted in the previous 10 years of specified crimes from working as a security screener or otherwise having unescorted access to secure areas of an airport.”

Similarly, Title VII includes a national security exception that permits an employer to decline to hire an individual because he or she cannot satisfy the federal security clearance requirements. In other words, if a security clearance is required for the applicant’s position, an employer may, in some circumstances, deny employment based on the applicant’s failure to obtain a security clearance. That exception includes the following requirements:

- The position must be subject to national security requirements imposed by federal statute or executive order.
- The adverse employment action must result from the denial or revocation of a security clearance.

Thus, when analyzing this exception, employers should focus on the specific requirements of the position in question and the individual applicant’s circumstances to ensure that the job being sought is in fact subject to national security requirements and that the applicant cannot meet them. As a practical matter, employers should be mindful of the manner in which they learn of apparently adverse information and how they share that information within the enterprise.

It is also noteworthy that employers may generally consider the time it takes to obtain a security clearance, and by logical extension, the likelihood of delay. For instance, some research labs, defense contractors, and other entities may interview candidates in advance of hiring or promotion to determine whether costly delays may occur in the investigation and adjudication of an individual’s clearance. By analyzing possible security concerns before hiring candidates, employers may save time, money, and resources. But employers must be careful that the apparent adverse information does not lead to possible claims such as defamation or discrimination.

The EEOC’s 2012 guidance references its 1989 guidance that includes an unpublished EEOC opinion stating an employer did not violate Title VII when it failed to promote a naturalized US citizen from Yugoslavia, even though he was the most qualified applicant for the promotion. The EEOC determined the decision was a legitimate exercise of business judgment because it would have taken from six months to a year for the employee to receive the necessary security clearance. The EEOC noted that “no one from within the company was promoted to the position, the employer ultimately hired persons who already had the required security clearance, and there was no evidence that applicants of other nationalities received more favorable treatment in securing the position.” The 1989 guidance included another example:

> Z company loses a senior scientist two months before the deadline on a large defense contract with the federal government. In order to meet the contract deadline, Z must hire a replacement scientist immediately. Statutes dictate that persons working on defense contracts of this nature have a security clearance. CP, a woman, is selected as the most qualified scientist for the position. Z’s security specialist looks over CP’s security clearance forms and

discovers that CP has relatives living in a communist country. The security specialist knows from past experience that this will result in a lengthy security clearance process of greater duration than the contract. Because of that, Z hires a different qualified scientist, who is male and already has the required security clearance. Z's employment actions in this situation were based on legitimate nondiscriminatory reasons and thus do not violate Title VII.

The FTC also limits the reporting period for background checks

The Fair Credit Reporting Act (FCRA) also imposes certain procedural limitations on background screening. When conducting such screening of an applicant, an employer often either conducts an in-house background check or hires an external agency to conduct one. When using external sources, if the employer chooses an external agency that's deemed a consumer reporting agency (CRA) — which sells criminal or other background history information to employers — both the employer and the external agency are bound by the FCRA, which is enforced by the FTC. Under the FCRA, employers must adhere to certain notification and time restrictions. Individual applicants as well as employees may also bring private causes of action for any violations.

Under the FCRA, the agency cannot report arrest records more than seven years old if those arrests did not result in entry of a judgment of conviction. In contrast, the credit reporting agencies can report convictions indefinitely. The agency must also exclude:

- Bankruptcies after 10 years;
- Civil suits and civil judgments older than seven years or until the governing statute of limitations has expired, whichever is the longer period;
- Paid tax liens after seven years;
- Accounts placed for collection or charged to profit and loss after seven years; and,
- Any other negative information (except for convictions) after seven years.

Reporting restrictions for arrest records do not apply to individuals who will earn "an annual salary which equals, or which may reasonably be expected to equal US$75,000 or more."

The FTC provides other procedural requirements for obtaining and using background information. These are beyond the scope of this article. Employers, however, should be aware of the many notice, procedural, and timing requirements of the FCRA as they do pose a trap for the unwary.

US state law restrictions

As noted above, the "Ban the Box" movement has gained considerable momentum in the past few years. The laws relating to criminal inquiries vary widely from state to state, thereby contributing to the web of conflicting rules for employers to follow. Employers should be aware of the applicable laws in each state in which their company conducts business, particularly for locations with a facility clearance. The following are examples from various US states, including the District of Columbia, of applicants' rights and what can and cannot be asked during the hiring process:

California: An applicant has a right to view the file that the CRA has with his or her information, and order a copy of the file, upon submitting proper identification (such as a valid driver's license, Social Security number, military identification card, or credit card). The applicant may order a copy of the file at CRA offices or submit a written request asking that a copy of his or her file be sent by certified mail

or for a telephonic file summary. The CRA will provide trained personnel to answer questions about information in the file including any coded information. The applicant may bring another person to a CRA office, but he or she must show proper identification. The legislation also prohibits employers from inquiring about expunged, sealed, or dismissed criminal records.

District of Columbia: It is unlawful for employers to "require the production of any arrest record or any copy, extract, or statement thereof, at the monetary expense of any [applicant]." To the extent such information is requested, it may only relate to convictions or arrests that have occurred within the prior 10 years.

Illinois: Employers cannot inquire into or use the facts of an arrest or criminal history record that has been expunged, sealed, or impounded as a basis to refuse to hire an applicant. Also, applications must contain specific language that informs applicants that they are not required to disclose sealed or expunged records.

Massachusetts: If an applicant contacts a company's HR department, he or she has the right to know whether the company ordered an investigative consumer report about them. The applicant also has the right to ask for a copy of any such report.

Virginia: An employer cannot require an applicant to disclose information about an arrest or criminal charge that has been expunged.

Washington: If an applicant submits a written request to a company's HR department, he or she has the right to a complete an accurate disclosure of the nature and scope of any investigative consumer report the company ordered about the applicant. The individual is entitled to this disclosure within five business days after the date the applicant's request is received or the date the report was ordered, whichever is later.

UK "Best Practices"

GENERAL

- Employers can't reject an applicant for a job because they've been convicted of an offense after its "spent" period — which is a term used to refer to a designated rehabilitation period set forth by the UK Rehabilitation of Offenders Act 1974 (ROA).
    - Some jobs, however, are listed as exceptions to this rule and require a declaration of conviction prior to a job offer (i.e., nursing, childcare, and social work).
- If the position is not listed as an exception, applicants are not required to tell potential employers about spent convictions or cautions prior to receiving a job offer.

Custodial Sentence	**Rehabilitation Period (Spent)**
0-6 Months	2 Years
6-30 Months	4 Years
30 Months to 4 Years	7 Years
More than 4 Years	Never

CRB VS. DBS

- After the publication of the UK Protection of Freedoms Act 2012, the Criminal Records

Bureau (CRB) merged with the Independent Safeguarding Authority to become the Disclosure and Barring Service (DBS).
- The DBS is responsible for carrying out criminal records checks for candidates who are applying for jobs that are exceptions to the ROA.
- CRB and DBS checks are the same, however, receiving a CRB check does not mean that it's out of date.

DEVELOPING A POLICY

- Understand the parameters of the job in question.
    - Does it qualify for a DBS check?
    - Align aggressiveness of job search to meet company culture.
- Train managers, hiring officials, and decision makers to understand the restrictions of spent convictions.
    - Avoid judgments based on convictions in the rehabilitation period.
- Consider adopting Ban the Box procedures that eliminate the need to disclose criminal offenses based on preliminary job applications.

QUESTIONS ABOUT CRIMINAL RECORDS

- When asking questions about criminal records, know that certain questions are not required to be answered by the prospective employee prior to receiving an offer.

For more information, visit www.gov.uk/exoffenders-and-employment.

Recommendations for employers

The cost to a company of hiring an individual for a cleared position and then having that person not be able to obtain and maintain a security clearance is high — not only are there actual out-of-pocket costs, but there is also lost time, use of recruiting resources, incurred training costs, time spent on knowledge transfer, and the loss of other qualified candidates. Employers often have to find commercial, non-classified work for the individual while he or she waits to learn whether the US government will grant the clearance at the appropriate level such as SECRET or TOP SECRET.

Employers must ensure that hiring, promotion, and retention policies adhere to and use exceptions and defenses afforded under federal and state laws. Employers should keep the following points in mind.

Understand the purpose of the EEOC guidance

The overarching theme of the EEOC's guidance is that an employer may lawfully inquire and consider an applicant's criminal record in making an employment decision, but the employer must be able to show that the information is relevant to the job in question, and that denying employment on that basis is consistent with a legitimate business necessity.

Document, document, document

If you are relying on criminal background information to deny hiring, you should document your reasoning. For positions that require a security clearance, the extent and nature of an applicant's criminal history is, of course, highly relevant to whether the applicant will be able to obtain and maintain a clearance (and therefore satisfy the minimum job requirements). Employers must be mindful that the Facility Security Officer (FSO) will review the security clearance application for "adequacy and completeness." This means that the employer may become aware of certain adverse information such as an applicant's criminal history, including arrests.

Hypothetical problem: Financial background information

Employment background checks often return information related to prior financial problems previously faced by applicants. For example, prior bankruptcies, foreclosures, or liens may be reported. Under Adjudicative Guideline F titled Financial Considerations, employers may be required to report information about employees requiring clearance related to improper financial management, not meeting financial obligations, or other irresponsible indebtedness. However, experienced counsel can help present mitigating information to the US government that would avoid any adverse decision regarding an employee's security clearance. Employers need to individually weigh their business goals, timeframes, and risks in assessing how they make decisions regarding background information.

Analyze the EEOC national security exception

The EEOC provides employers with an affirmative defense, by way of the national security exception, as long as the position is subject to national security requirements and the adverse employment action results from the denial or revocation of a security clearance.

The EEOC guidance similarly provides that an employer may be able to use the defense when it chooses not to hire an applicant because the applicant discloses a criminal record that would delay or make it difficult for the applicant to obtain a security clearance. However, FSOs, attorneys, and HR professionals should consider the manner in which the employer informs the applicant that he or she did not meet the necessary requirements for the job.

In arguably borderline cases, the employer may be able to point to the potential time and cost associated with adjudicating a security clearance application as a business necessity that warrants excluding the applicant from employment. For example, if the employer believes in good faith that a dual citizen may ultimately receive a clearance, but the investigation and due process may take two years, the employer would typically be justified in passing on that applicant. Nonetheless, the employer may decide to hire the applicant because he or she could perform unclassified, commercial work for at least several years.

The employer should provide reasonable and clear guidelines on what is an unsatisfactory criminal history for a given position. Moreover, if a qualified applicant has a criminal history, the employer may attempt to obtain additional information so the employer can analyze whether the criminal history poses a significant security risk under the adjudicative guidelines.

Incorporate the EEOC's practical guidance

When making employment decisions, an employer should attempt to incorporate a consideration of the factors identified by the EEOC in the guidance discussed above, which support a finding of:

- “Job-related and consistent with business necessity;”
- An individualized assessment of the applicant; and,
- Implementation of “Best Practices” patterned on the list provided by the EEOC.

Determine whether FCRA requirements apply to your background investigations

Remember, the FCRA only applies to CRAs and the companies that obtain reports from these agencies. Accordingly, in-house background checks that do not use outside databases are generally not governed by the FCRA constraints (i.e., prohibiting arrest information beyond seven years). Even if an employer engages in the use of CRAs for its background checks, an employer should ensure that both it and the agency are following proper procedures, including the reporting of conviction records.

Ensure proactive measures are consistent with the objectives of the organization

The culture of the organization may determine how aggressive an employer and the leadership act in analyzing the security concerns within an organization. For example, some organizations may place a high priority on protecting confidential information such as trade secrets or classified information. Other organizations may prefer to take a less aggressive approach on pre-screening employees. Legal counsel should ensure that security professionals and HR understand the culture of the organization and that any proactive measures such as pre-screening are consistent with the organization’s objectives.

Know state and local laws

State and local laws vary widely with regard to limits imposed on background checks. Accordingly, employers should be aware of the applicable laws in each state in which their companies conduct business. The US government’s requirement for an insider threat program for cleared facilities may cause confusion for an organization that operates in multiple states.

Legal counsel should ensure collaboration among HR, security, and legal counsel

Refer hiring decisions involving arrest and conviction information to, or collaborate with, senior HR personnel and legal counsel who have the experience and knowledge to analyze the type of investigation required by federal, state, and local laws. Ensure that the security, HR, and legal departments consider the security clearance process, including due process that may be afforded to an employee. This includes the costly delays that might occur if the employee receives interrogatories (i.e., the US government’s request for additional information), a Statement of Reasons (i.e., specific allegations or security concerns against the employee), or a hearing before an administrative judge or officials from a three letter agency.

Don’t rush to report

Since the FCRA provides time for applicants and employees to challenge information provided in a background check, employers should be hesitant to immediately report security issues that are discovered in a background check of an existing employee, as it is covered by the FCRA. Identity theft, typographical errors, and simple human error in the background check process can sometimes cause the information in a report to be inaccurate. Rushing to report the information to the government might create unnecessary problems for employers. The regulations also state that employers with a facility clearance should not report adverse information that is based on “rumor or innuendo.”

See Department of Defense Manual 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) at §1-302; *Becker v. Philco Corp.*, 372 F.2d 771, 772 (4th Cir. 1967); *Mangold v. Analytic Servs., Inc.*, 77 F.3d 1442, 1449 (4th Cir. 1996); *Murray v. Northrop Grumman Info. Tech., Inc.*, 444 F.3d 169, 175 (2d Cir. 2006).

Conclusion

In today’s world, employers are increasingly screening the background of applicants before making a hiring decision or granting promotions. The consequences of failing to collaborate with legal, security, and HR departments during this process can create additional legal and practical problems. For instance, managers may make business decisions based on inaccurate information. If someone slips through the cracks, company leadership may question the effectiveness of proactive screening measures or even eliminate the measures implemented by seasoned security professionals.

Employers adhering to the EEOC guidelines will be in a position to provide an effective rebuttal to any subsequent challenges to employment decisions from the EEOC, FTC, or individual applicants. Additionally, security professionals should ensure that HR and legal departments are aware of any proactive measures such as prescreening that may have been implemented. This is particularly important with the US government’s requirement for insider threat programs for certain facilities.

At a minimum, by raising awareness with security, HR, and legal departments, facilities can move forward with insider threat programs and other proactive measures while remaining compliant with the appropriate guidance, laws, and regulations. HR personnel, legal professionals, and security officials must regularly communicate with each other to avoid running afoul of anti-discrimination rules on one side and federal security protocols on the other. And it’s not just about communicating with each other, but also ensuring you have seasoned outside resources to consult when questions arise.

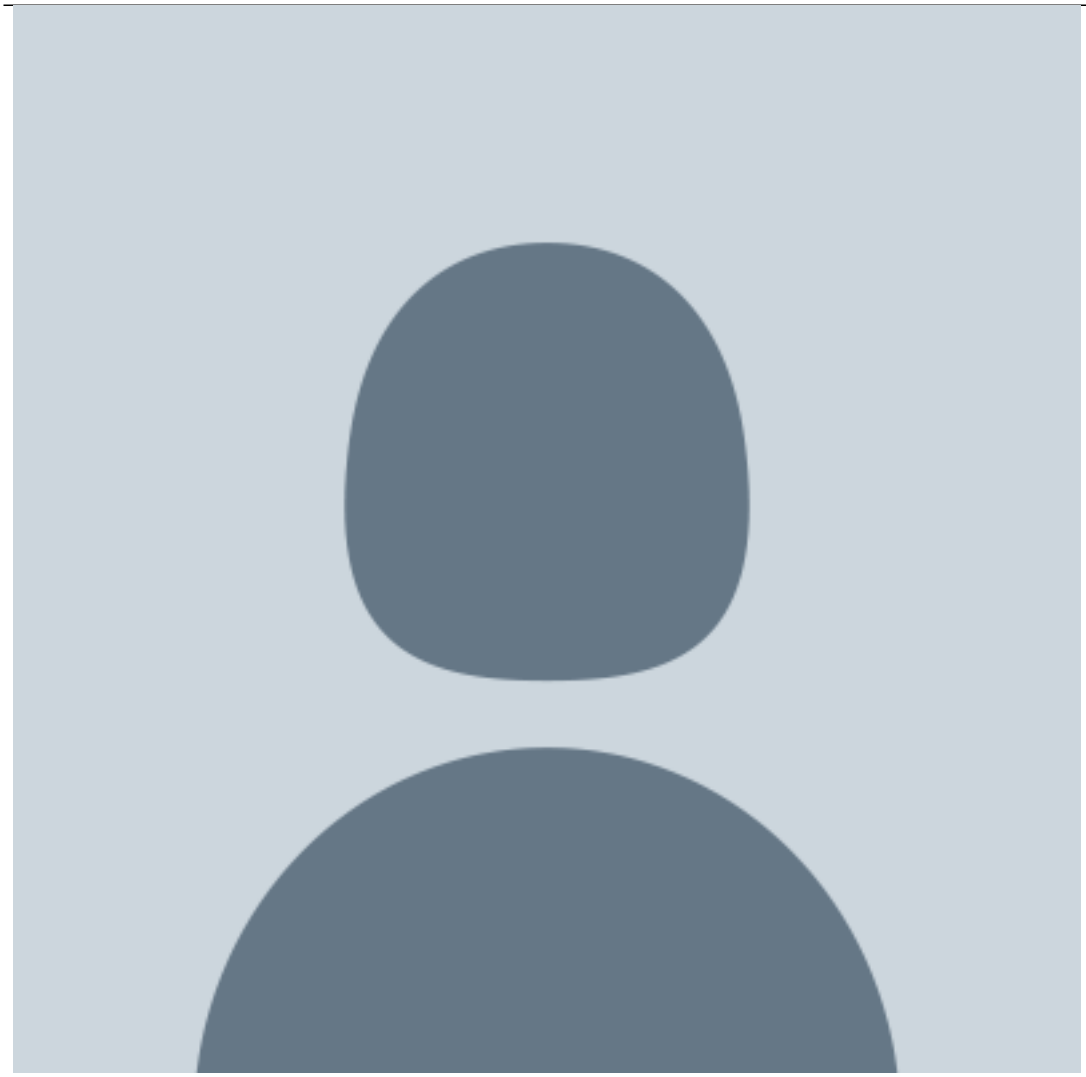
Erika Schenk

General Counsel and Vice President of Compliance

World Wide Technology

World Wide Technology is a privately held technology systems integrator, and she is responsible for legal compliance for the organization.

Brian Kaveney

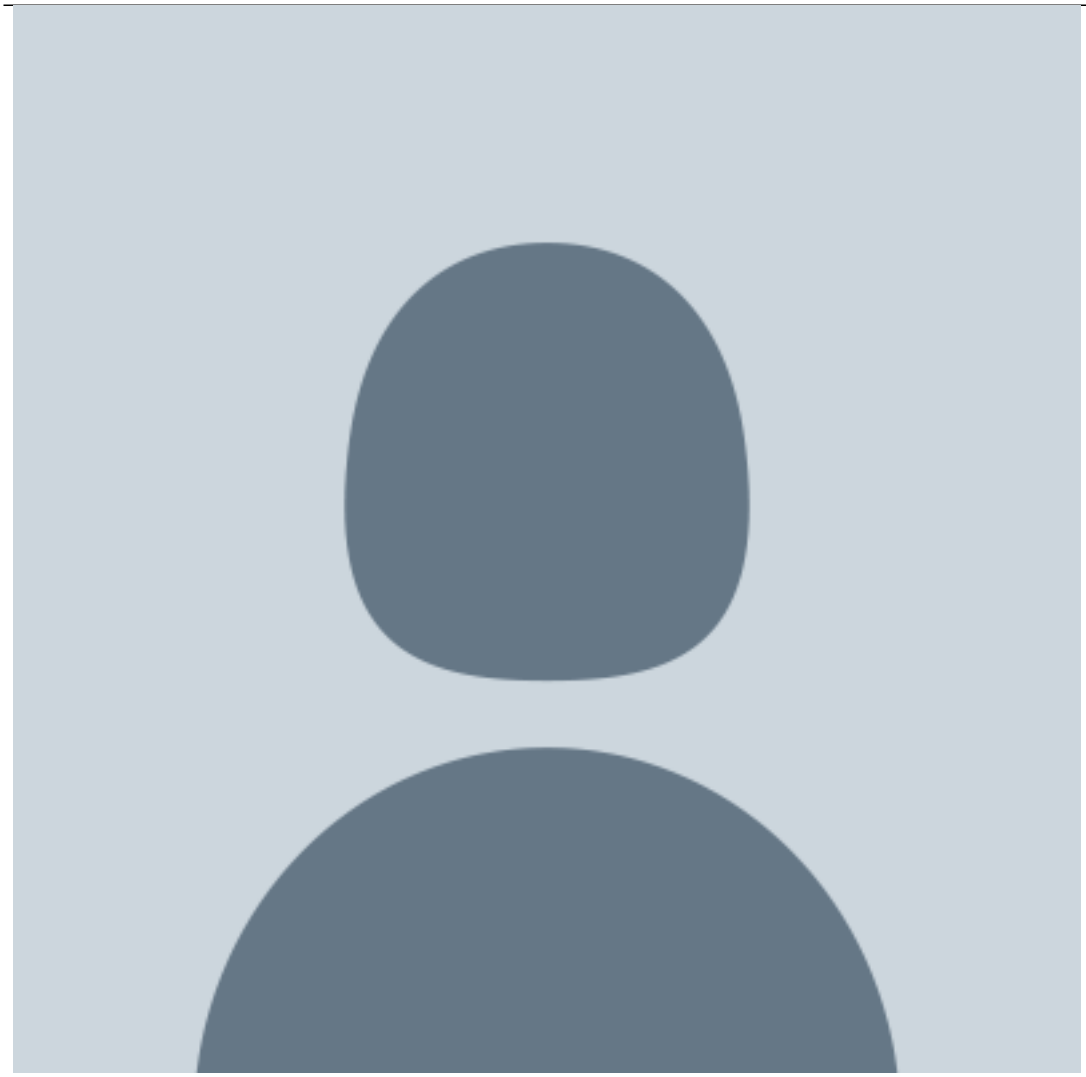


Partner leading the industrial security practice

Armstrong Teasdale LLP

Armstrong Teasdale LLP is a Lex Mundi member firm for USA, Missouri. He represents large public companies, universities, research labs, private businesses, and trustworthy individuals. He is a former US Marine officer.

Brad Bakker



Associate in the employment and labor practice

Armstrong Teasdale LLP

Armstrong Teasdale LLP is a Lex Mundi member firm for USA, Missouri. He provides a wide variety of consultation for employers and litigates employment matters in state and federal courts.