Guidepost

SECURITY CONSULTING

INDEPENDENT SECURITY STUDY

Reduce your exposure and offset the costs of an executive security program by conducting an independent security study.

The IRS has designated certain fringe benefits to companies as necessary for the safety of its employees, partners, and directors under U.S. Code Title 26 USC 132. To qualify, the IRS requires an independent third-party assessment to verify any legitimate security threat or concern. Performing an independent security study ("ISS") provides valuable insight into your company's risk environment for key corporate leadership and outlines the optimal treatment of the expenditures for the corporation and the executive receiving the fringe benefits.

Completing this assessment provides protection and safety for executives and may reduce tax liabilities and operational costs. [1]

A Guidepost ISS will assess the overall security posture for a variety of principals, including founders, CEOs, C-suite executives, and Board of Director members. These studies are performed in alignment with the requirements of Title 26 CFR § 1.132-5 – Working condition fringes, to determine whether there exists a business-oriented security concern based on objective facts and circumstances regarding the safety of the executive.

Our team has specialized expertise in assessing threats, risks, and vulnerabilities as well as providing recommendations, remediation steps, and best practices.

A GUIDEPOST INDEPENDENT SECURITY STUDY INCLUDES:

IRS 132 code requires consistent application of protection for all of the following conditions:

1. At the workplace
2. At the residence(s)
3. Traveling to and from the workplace
4. Traveling for business and/or personal reasons (including the use of corporate aircraft)

THREAT AND RISK PROFILE

An evaluation and analysis of the nature and credibility of the existing and potential threats to the executive. We review information across a variety of public and proprietary databases, and both traditional and social media to determine the availability of the principal's personally identifiable information. These data points are what adversaries may use to commit identity theft, leverage for extortion, and/or establish an individual's pattern of life. The executive's digital footprint is used by individuals or social activism groups for in-person approaches to harass, intimidate, harm, or embarrass.

Deep and Dark Web Searches

Title 26 CFR § 1.132-5 does not require deep or dark web searches. However, Guidepost also offers this service for clients who are concerned about their personally identifiable information, including usernames and passwords, exposed on the deep and dark web. The availability of this information primarily comes from data breaches, which contributes significantly to identity theft, medical insurance fraud, and tax fraud.

PHYSICAL SECURITY ASSESSMENT

Evaluation and analysis of the defensibility, architecture, electronic security systems, infrastructure dependencies, operations, staffing, communications, alarm monitoring, and response elements of the overall security posture at the principal's residence(s), primary office, and any corporate transportation hubs (i.e., aircraft hangars, watercraft docks, vehicle storage). The physical security assessments generally include the following elements:

- *Architecture*
- *Crime Prevention Through Environmental Design (CPTED)*
- *Technology*
- *Executive protection*
- *Security drivers*
- *Comprehensive review of security program policies and procedures*

ADDITIONAL SERVICES:

Cyber Vulnerability Assessment

Anonymous + Encrypted Communications

Personnel Recovery + Extraction

Identity + Reputation Management

[1] This material is not intended as tax advice and has been prepared for informational purposes only. You should consult your own tax advisors before engaging in any transactions.