

FOCUSPOINT RISK ADVISORY SERVICES

IRS 132 Compliance

Consulting Services Overview – A Personal Security Program Component

Reduce your exposure and off-set the costs of a personal protection program by engaging FocusPoint International to conduct an I.R.S. § 1.132-5 security assessment.

According to the I.R.S., if a bonafide business-oriented security concern exists, a company may exclude certain expenditures related to an employee. Some examples include:



Estate Security

Home Intrusion Detection Systems
Residential Security Guards
Safe Rooms



Special Risk Insurance
KR&E Insurance



Air Transportation

Commercial & Private Flights
Traveler Tracking



On-Going Threat Analysis
Security Analyst



Ground Transportation

Security Drivers
Chauffeurs



Office Security
Executive Suite Security



IRS 132 at a Glance

Corporate executives and high net-worth individuals within a recognized corporate structure often receive extraordinary fringe benefits not provided to other employees of that same recognized corporate structure that may be subject to tax. The Internal Revenue Code ("IRC") was amended in 1984 to include the term "fringe benefits" in the definition of gross income which must be treated as compensation includible in income under § 61 unless there is a specific statutory exclusion that applies to the benefit.

Under § 1.132-5, certain statutory exclusions exist if a "bona fide business-oriented security concern" exists. A "bona fide business-oriented security concern" exists only if the facts and circumstances establish a specific basis for concern regarding the safety of an employee. Treas. Reg. § 1.132-5(m)(2)(i).

Under Treasury Regulation § 1.132-1(b)(2), "employee" means: 1) any individual who is currently employed by the employer; 2) any partner who performs services for the partnership; 3) any director of the employer; and 4) any independent contractor who performs services for the employer.

No bona fide business-oriented security concern will exist unless the employer establishes to the satisfaction of the Commissioner of Internal Revenue that an "overall

security program" has been provided with respect to the employee involved. Treas. Reg. § 1.132-5(m)(2)(ii). An "overall security program" is one in which security is provided to protect the employee on a 24-hour basis. Treas. Reg. § 1.132-5(m)(2)(iii).

An overall security program will be deemed to exist in situations where the employer conducts and implements an "independent security study" with respect to the employee. Treas. Reg. § 1.132-5(m)(2)(iv).

An "independent security study" exists if the following are met:

- A security study is performed with respect to the employer and the employee by an independent security consultant;
- The security study is based on an objective assessment of all facts and circumstances;
- The recommendation of the security study is that an overall security program is not necessary and the recommendation is reasonable under the circumstances;
- The employer applies the specific security recommendations contained in the security study to the employee on a consistent basis. Treas. Reg. § 1.132-5(m)(2)(iv).

Meeting the Requirements of IRS 132

FocusPoint International (FocusPoint) is routinely engaged by corporations and family offices to conduct personal security assessments (PSA's) to meet the requirements of IRS 132. A PSA is typically conducted in order to establish a "baseline of threat" as the first step in establishing a practical (threatbased) "overall security program".

The PSA identifies current threat conditions and lifestyle dynamics to determine the resources required to establish and implement an effective and reasonable security program. As an unbiased, independent third-party consulting firm, FocusPoint's PSA satisfies the IRS requirements for tax credit under regulations § 1.132-5(m)(1).



The PSA™

The PSA is used to establish a baseline of threat. It serves as the backdrop from which a personal security program is pulled together and exercised when necessary. It is a roadmap of an individual's vulnerabilities and when leveraged correctly provides critical information in the response to emergencies. The PSA normally encompasses five areas of examination:



1) Threat Assessment



2) Residence Assessment



3) Office Assessment



4) In Town Travel



5) Out of Town Travel



1) Threat Assessment

In order to provide a sound basis for the decision making process involved in determining what configuration an overall security program should adopt, it is necessary to determine what potential threat conditions exist. Many factors affect the threat environment and changing variables often influence threat conditions. This module of the assessment encompasses an in-depth effort that identifies existing threat conditions and determines vulnerable areas in which a lack of deterrent or opportunity might exist. Interviews of key staff members and selected family members are conducted in order to identify historical threat conditions that will assist in future deterrence measures.

2) Residence Assessment

A detailed assessment of the primary residence is conducted during the review. This residence survey normally involves an interview and discussion with the key family member concerned and if applicable their spouse. This module is a very personal phase of the assessment as the evaluation extends to the family members private home. This module determines what existing security measures are in effect at the residence and examines the security program from both the equipment and the procedure standpoint. Information is solicited that will assist in identifying what, if any, existing intrusion detection system is installed in the residence and whether it is functional and being properly used. Other information is gathered that centers around procedures normally used when guests, maintenance personnel, or unknown callers present themselves at the residence. Procedures used to process mail and other deliveries are identified and examined.



A physical assessment of the residence provides two fundamental pieces of information: 1) the exact physical layout of the residence, including the configuration of any existing intrusion detection system, and 2) the determination of where the vulnerabilities of the residence are located. Normally these vulnerabilities are closely associated with the various avenues of approach and areas of cover and concealment as they are located on the residential grounds. In order to adequately determine this information two site visits are normally required: 1) during day light hours and 2) during hours of darkness. The visit during the hours of darkness can normally be accomplished immediately after dusk as this visit is focused on determining the existing lighting plan, and its effectiveness, for the residence.



3) Office Assessment

Office configurations, access control, evacuation, and other emergency response topics at the office are considered and addressed in this phase of the assessment. This module of the assessment focuses primarily on integration of the physical security program and any personal security program to determine how the protection staff concerned would interface with other aspects of the overall security program. Executive parking, or lack thereof, is also taken into account.

4) In Town Travel

Interview(s) are conducted with the principal and any key support staff that has visibility of and/or responsibility for the principal's in town travel. These interviews develop information pertaining to the normal in-town travel habits of the individual(s) concerned. Method of travel, times of travel, routes traveled and other routine travel habits are identified. Safety and security measures that are currently in effect, if any, would be identified and examined. A route analysis is subsequently conducted to identify potential problem areas or vulnerabilities, also known as "choke points". Potential safe haven locations as well as identification of emergency services that may be available are identified and discussed.



5) Out of Town Travel

This effort involves interviews similar to those conducted for the in-town travel assessment. The focus of this effort centers on out of town travel in both the domestic and international environments. Information is developed pertaining to frequency of travel, duration of travel, destination(s) and to the internal resources available to support the client with this travel effort. The process of arranging travel, from conception of a travel itinerary to completion of the travel is examined, and will include identification of communication capabilities that client personnel may have with the principal during travel times.



This module of the assessment also includes determining how information pertaining to potential travel itineraries is controlled and disseminated. Information pertaining to the usual configuration of accompanying staff and or family members is developed as well as information pertaining to how the accompanying staff or family members is configured during the travel. Lodging and transportation arrangements during out of town travel is identified and evaluated. Existing security related procedures or written material relating to travel security issues is examined and evaluated. The existence of traveler tracking tools and specialty insurance to address the risk of kidnap and/or extortion is identified and reviewed if applicable during this module of the assessment.



Insight & Direction

After research, interviews, and analysis, we compose an informative brief that provides the client with a clear understanding of the types of threats that exist and subsequent direction on how to protect and mitigate personal risk to an acceptable level.

Observations made during the assessment are highly confidential and will be delivered through pre-designated channels to the client. Discussion of observations encourage interactive participation by the client and enable them to be active participants in the assessment process. Recommendations on how to correct or modify observations made to safeguard the client are provided in the final deliverable and serve as the basis from which certain expenditures are excluded under IRS 132.

The final 132 Assessment (PSA) report is an easily understood document that addresses both macro and micro security concerns. Upon conclusion of the assessment, a comprehensive report is generated which reflects exhaustive analysis and detailed observations and provides sound, justified recommendations with realistic timelines on how to improve or correct an identified vulnerability or deficiency under the threat estimate. As an independent 3rd party review FocusPoint's PSA provides realistic recommendations based on industry best practices. FocusPoint leverages decades of experience and a proven methodology based on U.S. federal protective doctrine to conduct the PSA.

To learn more about IRS 132 Assessments and FocusPoint's PSA consulting service, please contact us at (866) 340-8569 or email us at info@wwfocus.com.



SECURITY

RISK



FOCUSPOINT®

Our People | Your Peace of Mind™