Background Checks

April 13

2012

This document contains guidance with respect to the conduct of background checks by Private Maritime Armed Security Companies. It is intended to provide guidance and advice to those seeking to address issues regarding this challenge but is not intended to provide legal advice.

IAMSP-2011-02-PRSC-001 v1.3

Notice and Disclaimer

1. The International Association of Maritime Security Professionals (IAMSP) is a volunteer, non-profit professional society that seeks to raise the level of conduct within the maritime security community.
2. The Association does not accept or undertake a duty to any third party because it does not have legitimate authority (i.e. the force of law) to enforce its own standards. Nor does it assume a duty of care to the general public, because its works are not obligatory and because it does not monitor the complete use of them.
3. IAMSP disclaims any liability for any personal injury, property damage or other damages of any sort that may arise directly or indirectly from the publication, use of, application or reliance upon this document. IAMSP disclaims and makes no claims of guaranty or warranty, express or implied, as to the completeness or accuracy of the information in this document.
4. Those using this document should ensure that they undertake their own due diligence and, in speaking with legal counsel, ensure that such legal counsel is given full, clear, and honest representation of the needs being met. Those consulting with this document should also consider examining other sources for the purposes of comparison or additional views that may not be covered in this document.
5. This document is provided as a guideline that members and others may consult when seeking to address issues associated with the conduct of background checks.
6.

Change Control

Serial	Date	Change	By	Comments
1	03 April 2012	Initial Draft	McDougall	Start
2	13 April 2012	Comments Round 1	McDougall	Comments submitted back via email
3	21 April 2012	Comments integrated and out	McDougall	Comments via email

Foreword

7. This foreword is considered an introduction to the IAMSP and is not considered to be part of the development process.

About IAMSP

8. The International Association of Maritime Security Professionals (IAMSP) was founded in 2010 as the result of a perceived need by a number of private entities to raise the level of professional conduct within the maritime security industry.
9. The Association is a not-for-profile, volunteer organization.
10. The IAMSP seeks to address a broad range of issues associated with the maritime security industry, ranging from the protection of vessels and platforms operating at sea and seaports.
11. The IAMSP is an inclusive organization, seeking to build strong relationships between likeminded organizations. It is the belief of the IAMSP that such alliances build stronger voices and further the ability to build capacity within the industry.

Contributing Members

12. The following members were involved in the development of this standard:
    a. Ioannis Chapsos
    b. Deborah Donnelly MA FCGmA ABCP
    c. Laura Hains MA CPP
    d. David Stone MA MSc
    e. Allan McDougall BA BMASc PCIP CMAS CISSP CPP
    f. Ingo Wamser RA/FAStr
    g. Jeff Woodruff CD CAS

Revision History

13. This document is the first version of this standard but is based upon research that includes peer-reviewed documents from 2010 and 2011.

Standard Designation

14. This standard is designated as IAMSP-2011-01-PRSC-001 where
    a. 2011 refers to the originating body,
    b. 01 refers to its applicability to ships,
    c. PRSC referring to the Personnel Screening, and
    d. 001 refers to its being a general topic.

Keywords

15. Use of Force, deterrence, armed security personnel, lethal, less-lethal, non-lethal, escalation

Table of Contents

Special Consideration

Personnel Security Screening is highly influenced by national laws and practices. These will be linked directly to the company requesting the screening, any entity performing work on behalf of that company and the individuals involved. Often this interaction is complex, if not complicated, and it is strongly recommended and advised that this kind of effort only be established with specific inputs from competent legal authorities.

Individual nations may have specific laws that can have an impact on the ability to conduct security screening. In Canada, for example, a fingerprint check may be requested to confirm the identity of an individual before record information is released. In Germany, a "private" request may only include judgments of over 3 months or the financial equivalent. Those conducting these checks should, as a matter of routine, request that any specific limitations regarding the information being provided or the checks be identified at the onset.

Similarly, the conduct of checks may be hampered by more mechanical factors-such as the individual's national identification standards, the ability to send mail, the ability to communicate with personnel and so forth. These factors can have a significant impact on the ability on the organization to conduct their checks in a timely manner.

International conventions and national laws often ensure that individuals are not subject to unreasonable searches or intrusions into their private lives. Similarly, they often assure individuals that they are entitled to due processes that are free from discrimination. Those establishing these programs should ensure that these kinds of factors are taken into account.

This kind of program can often pose a significant legal or civil risk to a company. While this document is put together based on sound research and specifically reviewed by persons competent in the field, the Association informs the readers of this document that this kind of risk may exist and strongly encourages them to ensure that they have sought appropriate legal advice with respect to their own operations, operating areas and specific requirements. The reader agrees to hold harmless the Association in the use of this guidance.

Scope, Summary, and Purpose

Scope

16. The *Conduct of Background Checks* is not intended to cover all aspects of the personnel security screening but is rather intended to address what are seen as key points. It is intended to take a broad and international focus.
17. It is recommended that persons using this standard consult with legal counsel with appropriate competence and experience in the domain if seeking to develop internal policies regarding the conduct of background checks. Of note, companies should consult legal with respect to (at least) the following issues:
    a. Privacy legislation in the applicable jurisdiction,
    b. Human Rights legislation in the applicable jurisdiction, and
    c. Accessibility legislation in the applicable jurisdiction.

Summary

18. The *Conduct of Background Checks* covers the following issues:
    a. General policies and standards defining requirements associated with the conduct of background checks
    b. Description of a sample background check
    c. Sample forms with respect to the conduct of background checks.

Purpose

19. The purpose of this document is to provide a foundation for those developing internal *Conduct of Background Checks* policies and procedures within their organization.

Terms and Definitions

20. ***Administratively Downgrade*** – The decision used to lower or reduce the level of an individual's completed security screening so that the individual's effective clearance is lower than what was originally completed. This process is used only when the individual no longer requires access to the higher level of sensitive materiel, information or operations. It is not considered to be an action against the individual, simply a reflection that the individual no longer works with the higher level of sensitivity involved (e.g. an individual no longer requires access to classified material and, as a result, his or her level of clearance is reduced so that he or she is no longer considered cleared to have access to it).
21. ***Administrative Suspension*** – the decision used to remove an individual's security clearance and thereby remove their ability to access sensitive information for a period of time based on the individual no longer needing access to sensitive material (e.g. an individual proceeds on a period of leave during which they will not be called back to work).

22. ***Adverse Information –*** Consists of information or data that would, when considered in the security screening process, lead to a decision to deny or revoke a clearance.
23. ***Background Check*** – the qualitative assessment of an individual's character through an examination of his or her past actions, accomplishments, and held beliefs.
24. ***Background Screening***– the process of taking the results associated with background checks and comparing them to set levels established through an assessment of risk to determine whether or not an individual can be considered reliable and trustworthy with respect to a certain level or kind of access.
25. ***Cause*** – a term commonly used to describe information that comes to light that would result in a condition of reasonable grounds. An investigation for cause seeks to ascertain the credibility of the information that has come to light and, if the information proves to be credible, then there may be argued that probable cause exists with respect to re-opening the security screening.
26. ***Care and Control*** – the state of being constantly held, within reach or controlled in such a way that only the individual can gain access to the physical item or attempt its removal. This also includes ensuring that another individual cannot gain access to information through overt or commonly covert means (such as shoulder surfing, etc).
27. ***Consent*** –the clear indication of an individual that he or she agrees to allow an organization's duly appointed representative to conduct a security screening for the purpose of determining whether or not that particular individual can (himself or herself) be considered reliable and trustworthy with respect to being granted access to certain persons, assets, information and / or operations (as appropriate to the check being conducted).
28. ***Denial*** – the decision to not grant a favourable outcome to the security screening process (such as the granting of a clearance). This decision is generally taken in circumstances where it is determined that the individual, due to information received during the security check process, would pose an unacceptable level of security risk to the organization if he or she had access to sensitive materiel, assets or information.
29. ***Evidence*** – facts and materiel that is used to determine and demonstrate the truth of an assertion. To be entered into evidence, the facts or materiel must be pertinent, legally obtained and meet criteria that establishes that it has not been altered or tampered with in any way since the time it was discovered.
30. ***Identity*** – a designation used to distinguish a unique and particular individual, organization or device.
31. ***Incapacitated individual*** – an individual who has been determined as not being legally accountable for his or her individuals due to a diminished capacity or medical condition.
32. ***Minor*** – an individual that has not yet reached the age at which he or she is considered to be a legal adult.
33. ***Nation*** – a clearly bounded and defined political entity that has achieved international recognition. While the concept of "nation" is often used to define a social or cultural entity, it is not the intention in this case.
34. ***National Interest*** – the security and social, political, and economic stability of a state.

35. ***Natural justice –*** the principles and procedures that govern the adjudication of disputes between persons or organizations, chief among which is that such adjudication must be unbiased, given in good faith and that both parties are given the same information and level of access as the other
36. ***Normal person*** – an individual that has no medical or psychological condition that can exacerbate the injury associated with the application of force against him or her. For the defender applying force, a person may be considered normal unless the individual shows outward signs or indicators of the condition that could lead to the exacerbation of the injury.
37. ***Presumption of Innocence*** – the assumption that an individual is not guilty in a criminal sense and that the burden of proof is on the prosecution, which must collect and present enough compelling evidence to convince the adjudicating body of their fact. In this context, the individual can only be convicted of the crime where it can be shown beyond a reasonable doubt that the individual did, in fact, meet all the criteria associated with being convicted.
38. ***Probable cause*** – apparent facts discovered through logical inquiry that would lead a reasonably prudent and intelligent person to believe that a person has committed a crime, thereby warranting his or her prosecution.
39. ***Reasonable grounds*** – a series of facts or information that would lead a reasonable or prudent person to a belief that is greater than mere suspicion.
40. ***Reliability*** – the condition or state of an individual that he or she can be trusted to perform tasks and act in accordance with the legal and organizational norms of a community w
41. ***Resolution of Doubt –*** the process used by which the organization clarifies the circumstances surrounding information that may, or may not, be detrimental to an individual's ability to successfully undergo the security screening process. This may involve seeking additional information to fill in gaps or may involve seeking alternative views or explanations of information that has already been presented.
42. ***Revocation*** –The decision to overturn the decision to grant a security clearance. This is generally based on either a (1) discovery of adverse information that would lead to a clearance not normally being granted or (2) a mistake in the process that means that a clearance cannot be granted. Due to the significant sensitivity of this action, this decision is generally reserved for a higher level of management in the company.
43. ***Risk*** – the condition of uncertainty that can create exposure to undesired future events or outcomes. It may also be used to describe the condition of uncertainty regarding positive outcomes, although this is less common in the security lexicon.
44. ***Security clearance*** – indicates the successful completion of a security screening that includes all aspects of the Reliability and Suitability check as well as checks pertinent to the national interest. This generally involves the individual meeting one of three criteria associated with having access to "classified" levels of access.
45. ***Security screening*** – indicates a series of pre-planned checks to which the individual has given clear consent and that are wholly required in order to make the decision as to whether or not an individual can be considered trustworthy with respect to the level of access to assets, information, or operations associated with the screening.

46. ***Security safeguard*** – a physical, procedural, administrative or technical measure that is used to delay or deny access to an attacker.
47. ***Special Access Clearance*** – a series of checks that are used to determine the reliability and trustworthiness of an individual with respect to a narrow (limited scope) and particular kind of access. The Special Access security clearance is not used to offer a broad level of access to sensitive information, materiel or areas.

General Policies and Principles

48. General policies and principles are divided into three major sections. These are the following:
    a. Oversight
    b. Specific infrastructure and considerations
    c. Sample policies (Appendix A)

Oversight

49. Oversight refers to management's establishment, communication, monitoring and enforcement of its decisions. While it is important for an organization to have a Conduct of Background Check policy, the value of that policy is also heavily dependent upon management's commitment to ensuring that its organization adheres to that policy.
50. The following sections describe certain requirements that need to be met in their policy.

Internal Policies

51. The *Conduct of Background Check* policies must be endorsed by the senior management of the organization. Where the policy is developed by a functional group (such as a legal department) or an outside contractor, they must still be clearly endorsed by the company's senior management.
52. The internal policies associated with the conduct of background checks must be developed with the assistance of competent and appropriate legal guidance. To be considered appropriate and competent, the legal guidance must have relevant knowledge and experience.
    a. The conduct of background checks must comply with international conventions, national laws and regulations.
    b. The conduct of background checks must also take into account the cultural sensitivities of those undergoing the checks. It should be clear, however, that this does not give the individual the right to bypass the background checks or to attempt to diminish their credibility.
    c. Where there is a conflict between the background checks being conducted and a cultural element, the onus is on the individual to meet the requirements associated with providing clear and credible information that would have been generated by the check.
53. The internal policies associated with the conduct of background must be clearly documented and communicated to all those that may have to undergo the security screening process before they undergo that process.
    a. Clear communications requires that the individual understands the nature of the checks being conducted, their value and their outcomes.

b. The individual must indicate that they understand and give consent to the checks.
c. The onus is on the company to be able to clearly explain, in plain (non-technical / non-legal) terms the nature of the checks being conducted.

54. The internal policies associated with the conduct of background checks must also be periodically reviewed from time to time to ensure that they remain accurate and relevant to both the legal environment and operations of the organization. This is also to take into account changes in other requirements (such as international conventions).
    a. The background check itself should also be updated or reviewed periodically to ensure that information is kept up to date and to detect any changes in circumstances. The length of this update cycle is to be clearly communicated as part of the process of giving consent.
55. The internal policies associated with the conduct of background checks, if updated, must clearly indicate the nature of the revision, the individual making the revision, the authority upon which the revision was based, and the dates associated with the revision (decision and coming into force). Past versions of the policies are to be removed from circulation and marked to prevent their inadvertent use.
    a. Where an individual undergoes a background check and additional requirements for the same level of check are added, the file must be annotated to indicate if the additional check was conducted or is to be conducted the next time the screening process is updated.
56. It must be clearly understood that the individual (or the demonstrable and verifiable legal guardian of a minor) must authorize the organization to conduct the checks using clear and written consent at the initiation of the process. In this case, the following applies:
    a. The individual must be informed that the security screening is a condition of employment and that the failure to give consent will mean that the organization will not be able to complete the hiring process in his or her case,
    b. The individual must be informed of the specific nature of the checks to be conducted, the basis for their being conducted, and how they are conducted as part of the consent process.
    c. The individual must be informed as part of the granting of consent process that he or she will have an opportunity to explain any adverse information before a final decision is made, and
    d. The individual must be informed that he or she cannot be hired until after the security screening process is completed (if there is a favourable outcome).
57. It must be clearly understood that the company must also demonstrate that it has taken all reasonable steps to ensure that it has met the requirements of due diligence. A company, or its directors, cannot shed their accountability with respect to the protection of personal information and ensuring its appropriate use. This accountability is defined in the legal requirements of various nation states and is limited to taking reasonable steps to ensure the protection of that information.
58. The policy is to clearly define how the company intends to monitor decisions made involving the use of security screenings and the steps that will be taken should it be determined that adverse

information has been identified. The identification of a security screening issue is to include the internal notification of company officers, the notification of clients (if appropriate), and the notification of the Team Leader (if appropriate).

59. It should be noted that the decision to embark or disembark persons resides with Master.

Infrastructure

60. Companies rely upon personnel, assets and information to carry out their decisions. There are certain elements of the conduct of background checks and security screenings that are specific to each of these elements.

Personnel-related

61. All personnel within the organization must undergo the company security screening process before being given access to sensitive assets.
    a. The requirement for screening is linked to the asset or information being accessed and not the employment status of the individual. Where an individual from outside the company (such as a contractor, student or volunteer) requires access to an asset or information that would require a background check, the same conditions apply as though the individual were an employee.
62. The CEO may delegate the authority to conduct the security screening process, but must remain aware of the following:
    a. That he or she remains accountable for the process and its quality,
    b. That he or she remains accountable for the basis of the decision to delegate authority, and
    c. That he or she must take reasonable steps to ensure that the individual to whom the authority is delegated is appropriately trained, educated and experienced in the conduct of security screening activities.
63. Individuals involved in the decision-making process must be made aware of the following:
    a. That the information that they receive as part of the security screening process is to be held in strictest confidence and not distributed to those that are outside of the process,
    b. That they will be occupying a position of trust which has legal obligations to both the company and to the individuals who have provided personal information,
    c. The specific nature of those legal and regulatory obligations (particularly with respect to the collection, use storage, distribution, release and destruction of such information),
    d. The penalties associated with failing to adhere to or report failures in adhering to those obligations, and
    e. That any abuse of the trust that individuals have placed in them will not be tolerated and may also result in civil or legal action.
64. Individuals that perform functions associated with the security screening function must be able to demonstrate the following:
    a. Appropriate training in the process used,
    b. Appropriate training in the handling of sensitive information,
    c. Appropriate understanding of potential indicators of adverse information,
    d. Appropriate training in the resolution of doubt,

e. Appropriate training and experience in the conduct interviews and detection of deception,
f. Appropriate training and experience in risk management, and
g. Appropriate training in terms of the internal security screening process.

65. Individuals handling files associated with the security screening process are placed in a position of trust over sensitive assets that are often protected by law or regulation and are often highly personal in nature. As a result, the individual must possess the following personal suitability factors:
    a. Discretion,
    b. Tact,
    c. Trustworthiness / Loyalty, and
    d. Compassion.

Assets

66. All security screening equipment must take into account the need to protect any sensitive information (either being entered, stored, processed, deleted or displayed) against unauthorized disclosure, modification or loss of availability.
67. All security screening files are to be produced, maintained, stored, communicated, transmitted, transported, and destroyed with respect for the need for protection against unauthorized disclosure, unauthorized modification (in terms of additions, deletions or changes), or losses of availability. This is to include the following:
    a. An individual`s security screening file should be started at first contact with the individual and the screening program and should follow the individual for as long as he or she remains in the organization,
    b. Files are to be uniquely identified but should use a system that does not use the name of the individual (e.g. numbered file system),
    c. Files are to have a control sheet on which any individual making an addition, modification or deletion from the file indicates the specific change and basis for the change. These are to be signed off by the manager to ensure completeness and appropriateness,
    d. Files are to be stored in such a way as to protect against unauthorized disclosure, modification or deletion / removal. For physical files, this means ensuring that the file is stored in a locked cabinet that only the individual who has been appropriately delegated to perform work on the file has access. For electronic files, this means ensuring that all files are protected through appropriate means, such as but not limited to, encryption, password protection, limited groups and permissions, segregated systems or other technical means.
    e. Files are to be transported within sealed envelopes bearing the return address of the company's security screening organization (sender) and intended destination.
        i. When carried by an individual who has been delegated to conduct personnel security screening activities, carrying the envelope in a standard carry case is considered sufficient as long as the file remains under continuous care and control,

ii. When sent in the care and control of an individual who has not been delegated, the envelope is to be sealed in a second envelope or packaging material to protect the item against inadvertent disclosure should the package be damaged, and
iii. All movements of files must be recorded in terms of the date sent, reason for sending, destination and a confirmation that the sender has received the file.

f. Files being sent by post are to be handled in the following manner:
   i. As per being sent by an individual who has not been delegated,
   ii. Only using trustworthy messenger services, and
   iii. In a manner that assures that delivery can take place within an identified time frame and requiring a signature for receipt.

g. Files being communicated by email or similar electronic means are to be handled in the following manner:
   i. Individual files are to be backed up to prevent inadvertent loss,
   ii. Individual files are to be saved with a password to open and a password to modify,
   iii. Individual files are to be encrypted (programs such as IronMail and MEO are readily available),
   iv. The password used to open or modify the file are not to be communicated in the same message and should ideally be sent by another means of communication, and
   v. Individual files are to be sent to the specific individual requesting the file without carbon copies or blind carbon copies.

h. Files being retained after their last administrative use are to be sealed and then stored as per active files. The date at which the organization can destroy the file is to be clearly marked on the file.

i. Files slated for destruction are to be protected in accordance with the following:
   i. The date of destruction is to be verified as not having passed,
   ii. The file is to be verified with management as not being needed for any other purpose,
   iii. The certificate of destruction file is to be completed, but not signed,
   iv. The file is to be destroyed using shredding, burning or similar methods in the presence of a witness.

68. Storage containers used for personnel files are to be controlled by either key or combination in such a way that only those persons who have been delegated have access to the key or combination.
69. All equipment used to copy, print or destroy file information is to be verified as not having copies of information left in the file. If electronic memory is involved (such as a print queue), it is to be verified as no longer holding any remaining print or copy jobs.

Information

70. The company shall only request that information necessary to determine if an individual is reliable and trustworthy to perform their assigned tasks and reasonably foreseeable tasks. The security

screening process does not give management the authority to check for details regarding an individual that are not pertinent to the work being proposed or other corporate requirements.

71. The company shall clearly identify what information or kinds of information it is requesting from its personnel. This shall be part of the process associated with the individual granting the company consent to conduct the checks.
72. The company shall, when asked to provide the results of security screening checks, provide a copy of the process used to conduct the checks and the results of the decision made. It should include a clear document to indicate that the company conducted each and every of the required checks.
73. The company shall, if asked to provide the specific information regarding a check, require that the requesting organization submit a letter from the legal department of that company indicating that the request is legal, that it is for the individual`s benefit and that the information sent will be protected as per the sending company`s requirement to protect against unauthorized disclosure, modification or loss.
74. In cases where the company is being asked to provide police, financial, national services (military) or other information, the individual who`s information it is must be consulted and give consent. The individual is to be advised of the outside party`s identity, basis for the request and consequences of not sending the information.
    a. This does not preclude the ability of official law enforcement or investigative bodies from being able to access the information provided in the course of their authorized duties within their jurisdiction.
75. In all transfers of such information, a statement shall be included on the transmittal form that the company being sent the information is responsible for only using that information for one check, may not communicate the information any further, and may only retain that information for the minimum period necessary (providing confirmation of its destruction to the sender).

Threat and Operating Environment

76. There are two elements associated with environmental considerations. These are the following:
    a. Threat environment
    b. Operating environment or physical environment.

Threat Environment

77. Full file information is not to be retained or stored in areas that are considered to be at an elevated threat level unless measures determined by a threat and risk assessment are put in place.
78. The onus is on the individual being screened to identify any potential groups, nations, organizations or other entities that may pose a threat to the individual in this respect.

Physical or Operating Environment

79. Security personnel are to understand that any discussion regarding any other individual`s security screening that is not part of their assigned duties is considered to be inappropriate and subject to disciplinary action.
80. Security personnel are to understand that membership in the company does not afford access to security screening information except as part of the assigned duties. In cases of it being part of

assigned duties, the level of access is to the decisions only unless there is an immediate need to know specific contents in order to protect the safety of individuals (including the screened members).

81. Security personnel are advised that they should always ensure that physical measures taken to protect files take into account both surreptitious attacks and brute force attacks. They should also ensure a level of redundancy so as to protect against the information being exposed should the primary security safeguard fail.

Recommended Authorities

82. The following are the general sources of information pertinent to this effort:
    a. United Nations Universal Declaration of Human Rights
    b. Charter of the United Nations
    c. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)
    d. Comments from the UN Human Rights Rapporteur with respect to privacy and the recommendations to Legislative Assemblies
    e. The International Code of Conduct for Private Security Service Providers
83. The following are certain documents should be clearly understood:
    a. Any Bill of Rights, Charter of Human Rights or similar legislative document associated with the citizenship of the individual being screened,
    b. National legislation including the following:
        i. Rights to privacy
        ii. Protection of personal information and data (including electronic)
        iii. Access to Information or Freedom of Information

Procedures

84. These procedures are provided as guidance only. Companies and other entities may use these but assume full and sole responsibility for the procedures being used in this respect.

Identifying Requirements

85. Identify the specific requirements of the job with respect to sensitive assets, based on (but not necessarily limited to) the following:
    a. Controlled assets (weapons, ammunition, communications equipment, etc),
    b. Confidential or proprietary information (file rooms, electronic, storage spaces, etc)
    c. Computer or communications systems, and
    d. Physical spaces that hold any of the above.
86. Identify the specific requirements associated with each kind and level of access. This should also take into account specific licensing requirements associated with the individual's citizenship and the proposed areas of operations.
87. Consult the Threat and Risk Assessment to determine if elevated controls are required.

88. Collate all checks required onto a single source for the position and location (may be used for similar positions).
89. Ensure that any job postings or similar communications clearly indicate that a security screening will be required (if equivalent clearances are possible, identify them at this point) as a condition of employment.

General Process

90. Have the individual, as part of the initial contact, sign the consent form for the conduct of checks, including signing that he or she understands the nature of the checks being conducted and consents to them (verify that they do not possess any of the alternatives—if they do, it may save time and expenses if it is appropriate for use),
91. Conduct the checks required, documenting the date of the check, the name of the individual who conducted the check, the method used to conduct the check and the outcome of the request. All information is to be filed as soon as received.
92. Where information is lacking, return a request to the individual to provide the information or an explanation as to why it cannot be included (and a means of verifying the veracity of this claim), ensuring to treat the communication as being sensitive in nature,
93. Submit the request to the reviewing officer who will review the submission,
94. Where there is a lack of clarity, conduct the resolution of doubt interview,
95. Collate all information and identify any particular areas of potential risk that may be unacceptable,
96. Make the decision to grant or deny the clearance. If the individual has failed to meet minimum information requirements, this may also lead to a determination that the process cannot be completed.
97. Take steps appropriate to the decision:
    a. Granted – then have the individual complete the acknowledgement certificate,
    b. Unable to complete – have the individual acknowledge that they understand that if they submit the required information, the process can be completed but that is their decision not to submit,
    c. Deny – inform the individual of the decision and their avenue for appeal.

Guidelines

98. Companies should ensure that their personnel security screening policies and practices are reviewed by an outside party not less than every five years.
99. Companies should consider integrating verification that unnecessary files are destroyed as part of their Quality Management or Assurance standards.

Revision of Standard

100. This document shall be reviewed at least annually and upon any of the changes indicated in this document.

Appendix A - Sample Policies and Procedures

101. The policies below apply to the hiring, monitoring, dismissal and release of employees and the effects that these processes have on the security clearance held by an individual.

Policy 1 – Delegation of Screening Responsibilities

102. The CEO delegates the responsibility for the day-to-day operations of the background check process to the Director responsible for <<corporate name>> including the following tasks:

a. Making recommendations regarding the level and nature of checks to be conducted,
b. The communication of the need of applicants and personnel to undergo security screenings,
c. The gathering of an individual's consent,
d. The creation, maintenance, review and destruction of files,
e. The conduct of checks,
f. The decision to grant a security clearance where no adverse information is determined,
g. The making of recommendations regarding the decision to grant, deny, revoke, or suspend a clearance where adverse information is discovered,
h. Administratively downgrading an individual's clearance where warranted, and
i. The day-to-day operations of the active monitoring program.

103. The CEO holds the responsibility for certain tasks within the personnel security screening process, including the following:

a. Approving the level and nature of checks to be conducted based on the recommendations of the individual delegated above,
b. Supporting the need and requirement for individuals to undergo the security screening process,
c. The setting of the period for which files will be retained,
d. As appropriate and contingent upon no conflicts being discovered with international, legal or regulatory requirements, the granting of a security clearance where adverse information is discovered,
e. The making of the decision to deny, revoke or administratively suspend a security clearance, and
f. Ensuring that appropriate support for the day-to-day monitoring program is included in the overall structure of the company.

104. Each individual who is delegated tasks associated with the conduct of checks or having access to the personal information of another employee as a result of tasks associated with the background screening process are advised and must acknowledge their understanding in writing the following:

a. That the use of any check or procedure for personal use or gain is forbidden,
b. That seeking access or accessing an individual's personnel security screening information without it being part of the routine day-to-day operations or appropriately delegated functions is forbidden,

c. That communicating information gathered within the personnel security screening process for any purpose other than those explicitly authorized and delegated by the company is forbidden.
d. That the employee understands that they are being put in a position of trust and responsibility that carries with it an obligation for discretion, tact, trustworthiness and compassion. Should it be determined that the individual fails in these aspects or fails to uphold the corporate principles in this respect is grounds for immediate and unconditional re-assignment or termination, as appropriate to the seriousness of the breach.

Policy 2 – Setting of Background Check Requirements

105. Background checks shall be set based on the following:
    a. The need to confirm the identity of the individual,
    b. The need to confirm whether or not any criminal record information exists,
    c. The need to assess the potential for compromise or inappropriate behaviour due to financial condition,
    d. The need to assess the potential for compromise or inappropriate behaviour due to features of character,
    e. The need to meet national legal or regulatory requirements,
    f. The need to meet international requirements,
    g. The need to meet the requirements associated with being given access to specialized equipment (communications, firearms, etc).
106. Suitability checks integrated into the background security screening may, as appropriate, also include testing for the following:
    a. Substance abuse,
    b. Psychological stability,
    c. Physical fitness, and
    d. Performance under operational conditions.
107. When dealing with checks, specific screening targets should be identified when setting the requirements. These targets must be based upon the following:
    a. The specific check,
    b. The time span that is to be covered by the check, and
    c. The preferred outcome of the check, and
    d. The specific issues that would likely automatically disqualify the check.
108. The candidate undergoing the check is required to submit a history that includes the specific address (as per mailing) and how long they lived at that residence. The span of time that the candidate is asked to provide information for is often based upon the nature and level of check being conducted. The following lengths of time should be considered:
    a. Unarmed security- 5 years
    b. Armed security – 10 years
109. In many cases, the individual undergoing the screening may have been deployed or working away from home. In those cases, the individual should provide a narrative regarding to what

countries he or she did work or, in cases where such information cannot be released directly, the name of their employer who can vouch for his or her conduct while away.

110. In some cases, the individual may not be able to release the name of the employer. In those cases, the individual should attempt to make contact with their former employer, advising them of the background check, and asking if an arrangement can be made to have the screening company contact the employer in order as part of the screening process.

111. It must be clearly disclosed to the candidate that a lack of verifiable information will, in all but rare cases assessed on a case by case basis, lead to a decision that the background check cannot be completed. This does not constitute a denial, but the individual cannot be declared to have successfully passed the background check.

Policy 3 – Standards of Information

112. All claims made during the security screening process must be supported by documentation and verifiable by outside third parties (this is to be interpreted in terms of the quality of information, not that an outside party would be given access to the information). Documentation may include notes made by the company official conducting the check, including the name, organization, method of contact, time of contact and duration of contact.

Policy 4 – Requirement for Records and Retention of Records

113. All information and data used in the security screening process must be included within the security screening file except where that information is requested to be withheld by a law enforcement officer or member of a national investigative body.

114. The information contained within the security screening file must be clear and concise to the level that an outside third party can render a decision based upon it without seeking clarification or expansion.

115. Records shall be retained for a period determined by the commitments and requirements placed on the company. Generally, this will be for not longer than a period of seven (7) years.

Policy 5 – Conduct of Basic Checks

116. The following steps constitute a basic series of checks used to determine the identity and reliability of the individual. They are the following:

a. Verify that consent has been given by the individual for any checks to be conducted,
b. Verify the identity of the individual
c. Inform the individual that adequate information must be provided in order to reach a decision and without the decision the hiring process cannot continue. This is not to constitute a denial of employment, only that the hiring process cannot reach a decision in either direction until adequate information is received.

Identity Checks

d. Complete the checks for identity information through the following:
    i. double checks involving identification issued by a legitimate international or state body,

ii. a check that shows that they can receive routine correspondence (such as mail) at a location under that identity, and
iii. an ability to corroborate their history under that identity.

e. Only once the identity checks have been completed, should outside checks be conducted. This is to reduce the risks associated with conducting checks that would return no results because of no record information (because there is no person) as opposed to there is no record of inappropriate conduct.

Criminal Record Checks

f. Request that the individual undergoing the screening process voluntarily disclose any criminal record information. Before making a deliberation following this kind of disclosure, those conducting the assessment should verify with the authorities involved as to whether or not there are any restrictions or limitations regarding the information that will be returned (such as convictions only, convictions of a certain nature only, etc). Note the following (also refer to resolution of doubt):
    i. The candidate is to be reassured that the presence of a criminal record does not automatically prevent them from being screened (depending on the nature of the offence and the level of screening considered),
    ii. The candidate is to be informed that a failure to disclose information may be interpreted as an indication of the individual's future willingness to hide information from the company in the future,
    iii. The candidate is to be offered the opportunity to explain the circumstances surrounding the record information and for that information to be weighed upon its merit without prejudice,
    iv. The candidate is to be offered the opportunity to demonstrate that his or her behaviour towards the offence is such that it can be reasonably determined that the chance of the individual re-offending is minimal or reduced to acceptable levels, and
    v. The position for which the individual is applying, and other positions that the candidate may be offered as part of the normal operations of the company, are to be considered.
g. It should be noted that certain jurisdictions require different approaches to criminal records checks. Some of these may include the following:
    i. Entities that only allow information regarding convictions to be provided,
    ii. Entities that may require the completion of a privacy check (such as the individual providing fingerprints to confirm his or her identity)
    iii. Entities that may only allow the individual to request the information and provide a certificate of good conduct,
    iv. Entities that may only cover limited periods of time or geographic jurisdictions, or
    v. Entities that may not allow for the use of official state record information for the purpose of conducting administrative checks.

h. Proceed with the request through legitimate channels. These may include any one or more of the following:
    i. national law enforcement bodies that maintain a service by which employers can conduct checks,
    ii. private services registered with national law enforcement bodies that maintain a service (often these will come at a fee).
i. The return of the national checks may come back in a variety of forms, these include (but are not necessarily limited to) the following:
    i. *No criminal record information found* – leading to a conclusion that there is no pertinent record information for that individual in that area within the time period that records are generally held,
    ii. *An incomplete check* – where additional information (usually associated with positively identifying the individual) is required before record information can be released,
    iii. *Record Information Found* – indicating that the body conducting the check was able to positively and uniquely identify the individual and that criminal record information was found attached to that individual.
j. Criminal record information should take into account a broad spectrum, but should pay particular attention to the following:
    i. Heinous crimes – murder, etc
    ii. Violent crime – assault, etc
    iii. Transborder crime – smuggling, etc
    iv. Weapons offenses – ranging from possession to unsafe use, and
    v. Breach of trust – or similar kinds of offenses
k. Having received criminal record information, the resolution of doubt process would be initiated. This is, of course, contingent upon there being no applicable national law or regulation that would preclude the individual from participating in the industry.

Previous Military / Law Enforcement Checks

l. Request that the individual provide a copy of any pertinent certificate pertaining to military, paramilitary or law enforcement / first responder services. These include:
    i. Certificates (or other forms of documentation) in support of any training,
    ii. Certificate of discharge or separation (honourable / good conduct / etc)
    iii. Certificate (or other forms of documentation) in support of any activities that are specifically claimed.
m. In cases of military or law enforcement release, there are several different conditions under which an individual may have been released. It is important to note that these may have different impacts on the ability to hire the individual and must also be taken in the context of the individual's reasonable expectation of fair treatment (human rights) and privacy. These may include the following:
    i. Retirement – in terms of the individual having completed a full military career and drawing a pension,

ii. Release at end of contract – in these kinds of cases, the individual may have released at the end of a period of service due to a range of issues. The reason for not returning should be ascertained (and may be completely reasonable),
iii. Released in terms of services no longer required – in cases where the military formation could no longer employee the individual beneficially (non-medical grounds). In these cases, care should be taken to determine what the basis of this decision was through reference checks or similar mechanisms.
iv. Medical Release – in which case the company should ascertain whether or not the medical condition would preclude the ability to pass the minimum standards associated with being deployed into the environment. While this often raises concerns regarding human rights, those concerns are alleviated when the decision is being made to preserve the safety of the individual (and those around him or her) or for his or her own benefit / welfare, or
v. Bad Conduct Discharge – for disciplinary reasons. The basis for this kind of discharge is important to ascertain.

n. Request that the individual voluntary disclose any circumstances that he or she feels would likely interfere with his or her ability to operate in the environment or hold the position being considered. For example, if the position involves travelling to certain areas, the individual ought to disclose if there are any immediate connections between a member of his or her family and groups that may be considered controversial, subversive or criminal. In this particular case, it should be explained that the need to know is based on a combination of business requirements but also the need to be able to determine if the individual would require exceptional protection against reprisals, etc.

Medical / Substance Use

o. Medical and substance-use related checks are very important within the maritime environment. These should include, but are not necessarily limited to, the following:
i. Any allergies or similar reactions to materials should be compared against the operating environment,
ii. Any medication conditions that require specialized treatment or medication should be checked against the ability to gain access to that treatment or whether the medication is considered a banned / illegal substance at any of the ports of call likely to be visited,
iii. Any issues with the use of substances (ranging from caffeine and smoking through to actual substance abuse) that could result in both an adverse affect on the individual but could also lead to conditions exposing the client or security detail to additional risks.

p. Similarly, care should also be taken to identify any dependency that could, if left unattended, lead to the person's judgement becoming impaired or their physical ability to do the job become compromised. These must be balanced against human rights aspects, but taking into account that the need for compliance is not based on administrative

security but rather the safety of the individual, those around the individual or the vessel itself.

q. Medical dependencies do not necessarily have to involve controlled substances. Care must be taken to understand the operating environment and how a dependency can interact with an individual's ability to comply with security, safety and environmental requirements. Consideration, for example, may want to be put forward for the following:
    i. Smoking – particularly in terms of ships carrying flammable materials / cargo,
    ii. Caffeine- particularly in terms of its physiological effects, and
    iii. Supplements – particularly if used to regulate an underlying medical concern.
r. Issues associated with medical treatment also factor significantly in terms of coastal state issues. In hiring an individual that has an underlying and disclosed condition, there is a level of tacit acceptance to assure that the individual is protected (reasonably) in terms of conditions, treatment and ultimately final care.

Credit Bureaus

s. Where the individual may be required to handle cash or report on funds, a credit bureau or similar check should be considered. The purpose of this check is to provide information to assess the individual's reliability in meeting financial obligations and to determine if the individual is under a form of financial duress. It should be noted, however, that financial situations can be the result of several legitimate factors (divorce, medical bills, etc) and should be interpreted carefully, generally by an individual with training and experience within the credit industry.
t. The conduct of the credit check takes the following steps:
    i. Having received consent, the company contacts the credit bureau, providing the name, national identification number (such as a social insurance number) and date of birth of the individual.
    ii. The credit bureau conducts its checks and returns results back to the company.
    iii. The results are then interpreted by the company.
        1. Where the results show a reasonable level of debt (this will vary significant by circumstance), consistent and on time payments, the results may be considered favourable,
        2. Where the results show an excessive level of debt, consideration should be given to determining if additional controls would be required in order to prevent skimming or similar threats. This kind of threat may increase significantly where there are indications that the individual does not pay or is in significant arrears.
        3. Where the results show a sudden and inexplicable relief of debt, this should be clarified.

Policy 6 – Conduct of Loyalty Checks

u. Loyalty checks can take the following forms:
    i. Assessment of an individual's past involvement

ii. Assessment of an individual's strongly held beliefs
iii. Analysis and assessment of the individual when placed in moral and ethical dilemmas

v. Loyalty checks can also operate in terms of their adherence to the requirements, norms, values and ethics of any of the following:
i. their nation of citizenship,
ii. their professional affiliations,
iii. their social affiliations,
iv. previous employers, and
v. previous associates.

w. In the cases of loyalty checks, the goal is to assess whether or not the individual will make decisions that represent an appropriate adherence to the groups they are associated with. For example, if placed in a situation where the there is a decision made between losing some money in a contract or revealing state secrets, the individual understands that the revealing of state secrets violates the principle of trust associated with their nation of citizenship and this precludes the ability to avoid the loss as violating that trust is considered to be unacceptable. This can be tested using a number of mechanisms or through the following (in comparison to the concept of loyalty):
i. Having the individual define or describe the concept of loyalty,
ii. Having the individual provide information on a past instance where loyalty factored significantly and having the individual provide some tangible or verifiable support for that claim, or
iii. Testing in terms of asking the individual to describe his or her preferred courses of action given certain circumstances.

x. Results of a loyalty check may be interpreted in terms of the following:
i. A return that is in line with the concept of loyalty gives a baseline of assurance but requires that the individual be monitored for changes in circumstance (citizenship, marital status, etc);
ii. A return that leads to additional questions should be followed up upon until those questions are resolved; and
iii. A return that raises questions regarding the individual's concept of loyalty should be interpreted in terms of the individual potentially being the source of corporate challenges in the future, particularly if a conflict arises between the corporate needs and the individual's own personally-held beliefs.

Policy 7 – Active Monitoring

117. A background check provides a picture of the individual up to that point in time. Any background screening must include a method of monitoring the behaviour and condition of the individual if it is to remain valid in the future.

118. Active screening should, at a minimum, take into account the following:
a. any areas of interest or concern identified in the background check,

b. any core requirements / mandatory requirements associated with the background check, and
c. any combination of items that would, if brought together, pose a potentially unacceptable level of risk with respect to the conduct of the individual or liability to the company.

119. The active monitoring program feeds information into the same process as the resolution of doubt process and can lead to a decision to revoke, suspend or downgrade the background check (as applicable and appropriate).

Policy 8 – Resolution of Doubt

120. Individuals undergoing background checks are still entitled to fair and impartial treatment. While this is generally an ethical requirement, it is also enshrined in many national laws and also in the United Nations Universal Declaration of Human Rights (various Articles apply ranging from the right to be free from arbitrary interference with privacy, attacks upon reputation, etc).

121. An individual must be given the change to explain the context and / or specifics of any discovered information before any decision to deny, revoke, suspend or downgrade the results of a background check is finalized.

122. Before being declared "adverse information," the information must be clear in terms of the following:

a. the relevance to the decision to grant, deny, revoke or suspend the background check,
b. the relevance to the position at hand,
c. the time that has passed since the events involved and any indications with respect to the individual having changed behaviour, and
d. the individual's current feelings towards the information.

123. The following examples are provided for general information purposes only and should not be used as specific examples or to guide specific cases:

a. The relevance of the information and the decision regarding the background check is dependent upon the the linkage between the information found and any access the individual may have to operations, controlled assets, and personnel.
    i. For example, a check that shows that the individual was convicted for a moving vehicle violation may not be relevant to determining whether or not the individual can be trusted with information networks.
    ii. For example, a check that shows that the individual has been convicted of an offence that would normally preclude them being licensed to carry a firearm would preclude the individual from being granted the company's permission to carry a firearm.
b. The relevance of the information to the position at hand is whether or not the information discovered can be linked directly to the task.
    i. For example, an individual that is addicted to nicotine (chain smoking) may be precluded from tasks where smoking is forbidden for safety concerns / regulatory requirements unless he or she can demonstrate control over the habit.

ii. For example, an individual that was convicted for a motor vehicle offence may not pose an unacceptable level of risk if the task involved has no contact with motor vehicles or the operation of motorized equipment.

c. Consideration must be given to the time that has passed since the event and indications that behaviour has changed.

i. For example, a criminal record that indicates that the individual was involved in a bar fight as a youth may well be mitigated in cases where the individual has matured significantly and there are no other indications of acts of violence or convictions of a similar nature.

d. The individual's feelings towards the information being found should also be considered. In some cases, the individual's conviction may be balanced by an appropriate sense of remorse or regret over the events and an understanding that such events are not acceptable.

124. It should also be noted that information that may be considered adverse may be the result of conditions or situations that are explainable and legitimate in nature. The individual must be given the opportunity to explain the context of any information.

125. The resolution of doubt process has an element of sensitivity that must be respected. This includes the following:

a. Ensuring that the need to conduct the interview is communicated only to those persons directly involved in the process,

b. Ensuring that the specific details of the interview process are handled so as to prevent them from being inadvertently disclosed or released to those outside of the immediate process,

c. Ensuring that any interviews are conducted with respect to the privacy of the individual, and

d. Ensuring that before the interview takes place, measures are taken that allow for assisting the individual (in case of stress or distress) or the interviewer.

Policy 9 – Decisions to Deny, Grant, Revoke or Suspend

126. The decision to grant, deny, suspend, revoke or downgrade the results of a background check must be based on an adequate quantity and quality of information. This includes the following:

a. The quantity of information must cover at least the minimum time period to be covered without breaks in continuity, and

b. The quality of information must be of a level so as to allow independent, third party confirmation of facts without the involvement of the person being screened.

c. Where either of these two do not exist, the screening process is discontinued until such a point that both conditions can be met. This may involve management making a decision to allow for an alternate method of check that meets the requirements with respect to the quality and quantity of information needed.

127. All decisions and the basis for those decisions must be clearly documented and the information retained for a period of not less than one year.

128. All resolution of doubt processes are to be included with the decision.

129. The decision to deny, revoke, suspend, or downgrade the results of a background check must be reviewed by a delegated officer in the company before being made official or finalized.

130. The company must maintain a mechanism by which it can impartially review decisions to grant, deny, suspend, downgrade or revoke a background check.

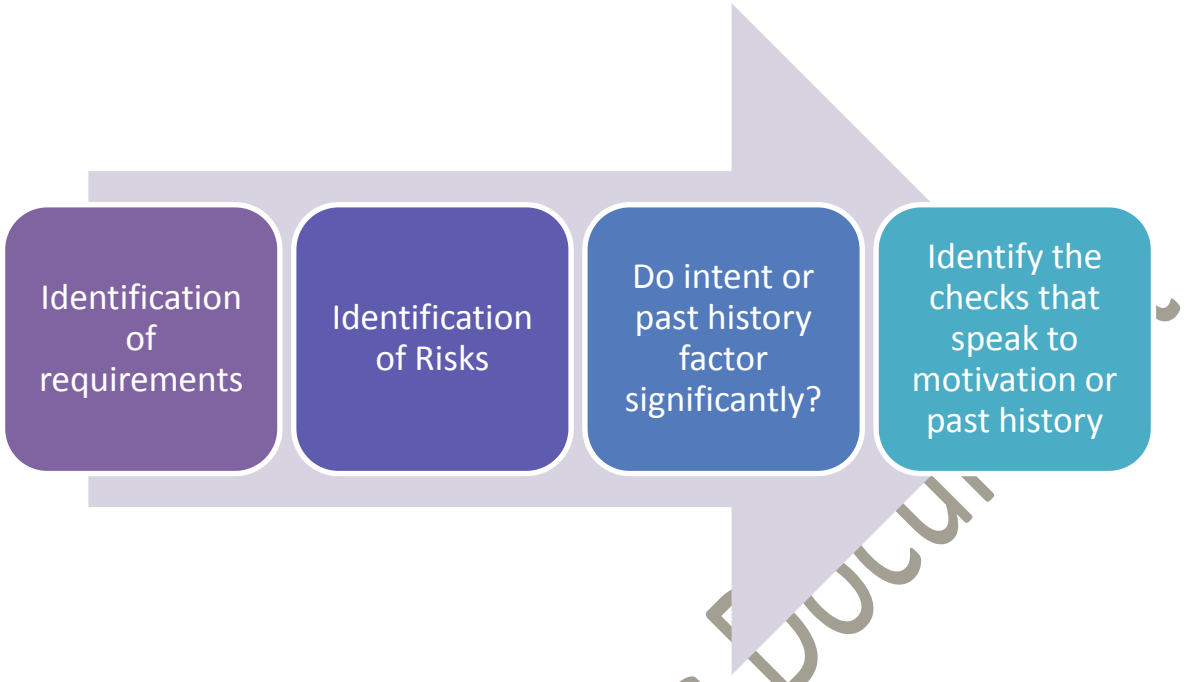
Policy 10 – Appeals

131. The appeal process must operate independently of those that made the decision to deny, revoke, suspend or downgrade the result of the background check.

   a. This appeal process provides recommendation to management, but does not require management to accept the decision to overturn a decision made by the delegated officer.
   b. In all cases, management's decision with respect to the appeal is to be clearly documented, including the basis for the decision.

132. A company's appeal process does not preclude an individual from seeking remedy if he or she believes that he or she has been unfairly treated.

Annex B – Integration of Personnel Background Checks into Security



133. Step 1 – Identification of Requirements
    a. Regulatory – based on national requirements (legislation, regulation, licensing)
    b. Agreement – based on agreements that require certain checks be conducted
134. Step 2 – Identification of risks
    a. Identify risks that require an individual to have intent
    b. Identify how that intent would manifest itself in past actions
135. Step 3 – Do intent or past history factor significantly?
    a. Does the event itself link clearly to information that would be discovered by a check?
    b. Does the motivation to commit an attack (etc) link to one of the specific checks?
    c. Is there a past history of the attacker using a specific or range of methods to attempt to convince somebody to perform the act on its behalf?
136. Step 4 – Identify the full suite of checks
    a. Each check should be able to link to the able to link to the above.
    b. For example, the threat of theft (petty) may be directly linked to cash handling perspectives. A criminal record check involving crimes of this nature (past history) and a credit bureau check (motivation) may be warranted in this context (in addition to basic identity checks).
137. Step 5 – Monitor for changes in circumstances
    a. The goal of the organization should be to conduct its affairs to prevent these kinds of circumstances from arising and also detecting if the individual is becoming involved in, susceptible to, or caught in situations that could lead to these kinds of circumstances.
    b. Care in this regard must be taken with respect to the appropriate balance of monitoring, supervision, corporate culture and employee rights (as applicable and appropriate).