IAEA NUCLEAR SECURITY SERIES No. XX-T

NST065

DRAFT

Step 8: Soliciting comments by Member States

Date: 23 January 2023

ESTABLISHMENT AND IMPLEMENTATION OF A TRUSTWORTHINESS PROGRAMME IN NUCLEAR SECURITY

DRAFT TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 20XX

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. As part of a nuclear security regime, there is a need for States to establish and maintain a trustworthiness programme to identify motivational factors (e.g. money, ideology, coercion, ego) that could motivate an insider to become an insider adversary. Such a programme aims at determining the trustworthiness of persons with authorized access to nuclear material and nuclear facilities; radioactive material and associated facilities and activities; sensitive information and digital assets, including those which may be accessed remotely; transport of nuclear and other radioactive material; and nuclear security activities in the areas of detection and response.

1.2. Recommendations on the establishment of measures to ensure the trustworthiness of personnel in order to protect against insider adversaries are provided in IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev. 5) [1]; IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [2]; and IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [3].

1.3. This publication provides technical guidance on how to effectively design and implement trustworthiness programmes for nuclear security.

1.4. The following list is an example, but is not an exhaustive list, of IAEA publications that discuss trustworthiness of personnel:

- The Amendment to the Convention on the Physical Protection of Nuclear Material [4];
- IAEA Nuclear Security Series No.7, Nuclear Security Culture [5];
- IAEA Nuclear Security Series No. 8-G (Rev. 1), Preventive and Protective Measures against Insider Threats [6];
- IAEA Nuclear Security Series No. 21, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control [7];
- IAEA Nuclear Security Series No. 25-G, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities [8];
- IAEA Nuclear Security Series No. 26-G, Security of Nuclear Material in Transport [9];
- IAEA Nuclear Security Series No. 36-G, Preventive Measures for Nuclear and Other Radioactive Material out of Regulatory Control [10].
- IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [11].

OBJECTIVE

1.5. The objective of this publication is to provide guidance on establishing and implementing a trustworthiness programme for nuclear security based on preventive and protective measures against the threats posed by insiders.

1.6. This publication is intended to be used by competent authorities, licence holders (operators) and other stakeholder organizations with responsibilities for the security of nuclear material or other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage or in transport. This publication could also be useful to stakeholders who are involved in the detection and response (e.g. law enforcement, customs officials, border security) to nuclear and other radioactive material out of regulatory control.

SCOPE

1.7. This publication describes measures that can be used to perform assessments and determinations of trustworthiness for individuals, and monitor the ongoing reliability, integrity and honesty of these individuals. The publication provides information on granting access authorization to nuclear material, other radioactive material, associated facilities or associated activities, sensitive information, and sensitive information assets, which includes information that can be accessed remotely. It also demonstrates how the trustworthiness programme is intended to be part of defence in depth for nuclear security.

1.8. This publication does not describe in detail how a State should implement the trustworthiness measures or gather information to support trustworthiness assessments, since the implementation of these measures depends on national legislative and regulatory requirements. Since trustworthiness programmes can vary from one State to another, this publication does not prescribe one way of implementing a trustworthiness programme, but rather presents guidance based on examples of good practice.

STRUCTURE

1.9. Section 2 provides an overview of a trustworthiness programme, outlining the benefits, methodologies for determining trustworthiness and the interface with nuclear security culture programmes. Section 3 examines the role of the State, designated competent authorities for trustworthiness asssessments and determinations, the licence holder, individuals and other stakeholders. Section 4 describes the implementation of a trustworthiness programme using a graded approach. Section 5 addresses the establishment of criteria for conducting trustworthiness assessments and making trustworthiness determinations. Section 6 describes processes for the implementation of a trustworthiness programme. Section 7 describes maintaining records for a trustworthiness programme.

Section 8 describes the process for granting an access authorization, suspending an access authorization, revoking an access authorization and reinstating an access authorization. Section 9 provides information on the protection of individuals subject to a trustworthiness programme. Section 10 describes trustworthiness programme reporting criteria. Section 11 describes audits and inspections of a trustworthiness programme.

2. OVERVIEW OF A TRUSTWORTHINESS PROGRAMME

2.1. Paragraph 3.14 of Ref. [1] states:

> "Taking into consideration State laws, regulations, or policies regarding personal privacy and job requirements, the State should determine the trustworthiness policy intended to identify the circumstances in which a trustworthiness determination is required and how it is made, using a graded approach. In implementing this policy, the State should ensure that processes are in place to determine the trustworthiness of persons with authorized access to sensitive information or, as applicable, to nuclear material or nuclear facilities."

2.2. Trustworthiness is the characteristic of an individual who behaves consistently — according to cultural, ethical and legal standards — with honesty and integrity, particularly in situations where the individual is not aware of being observed.

2.3. A trustworthiness assessment is the process of gathering the appropriate information (see Table 1) based on the access an individual needs to nuclear material, other radioactive material or sensitive information. The trustworthiness assessment results in either a positive or negative trustworthiness determination of an individual's behavioural indicators of reliability, integrity and honesty. A trustworthiness determination is based on information known at a particular point in time and is to be supported through ongoing assessments (e.g. self-reporting or changes in circumstances), oversight by managers and security departments, a behaviour observation programme and a nuclear security culture that encourages appropriate behaviours and the reporting of concerns (e.g. zero tolerance of harassment and bullying by peers or managers, reporting hotlines).

2.4. A trustworthiness assessment is a preventive measure intended to reduce the insider threat. Trustworthiness assessments to identify undesirable characteristics can be difficult because the intent and motivation (e.g. money, ideology, coercion, ego) of an insider adversary are not directly observable. Although the behavioural patterns of insider adversaries can vary significantly, aberrant behaviour can be easily observed. The observation of such behaviour is an important element of effective trustworthiness assessments, either providing evidence of a potential concern or, through further investigation, of contextually appropriate behaviour.

2.5. A trustworthiness programme consists of a set of processes for collecting information on individuals, assessing this information against defined criteria and determining whether trustworthiness has been established for these individuals. Trustworthiness programmes include initial assessments, periodic assessment, routine reviews, ongoing monitoring, special reviews, employee reporting and co-operation between departments or organizations (e.g. security departments, human resources, medical departments, supply chain organizations). Making a trustworthiness determination before granting an individual access to secure locations and sensitive information may reduce the potential risk from insider adversaries; however, this should supplement other control measures in order to be more effective.

2.6. The continuous implementation of a trustworthiness programme is a preventive measure that can serve as a deterrent to the attempt of malicious acts by insider adversaries given that individuals become mindful of being observed and modify their behaviour to meet the expectations of the licence holder. For this reason, if individuals demonstrate aberrant behaviour after receiving a positive trustworthiness determination, it could provide a possible indication of their intention to undertake a malicious act (see para. 5.5). Once such behaviour is reported, it is good practice to act according to predefined criteria, including the decision whether to revoke or suspend an individual's access until an inquiry can be undertaken to determine the next steps, as appropriate (e.g. return to work, rehabilitation or termination of employment).

2.7. While individuals tend to be consistent in their behaviour over time, behavioural patterns can change when an individual experiences significant or traumatic incidents. For this reason, a graded approach, established on the basis of risk assessments and available resources, should be used to determine the frequency and rigour of the scheduled trustworthiness assessments. Effective threat mitigation should include additional trustworthiness assessments on an 'as needed' basis, for example in the case of a significant or traumatic incident or observation of aberrant behaviour. Continued trustworthiness assessments during employment could identify individuals whose behaviour and characteristics negatively change over time.

2.8. Upon termination of employment, an individual's access to the premises and assets of the licence holder should be immediately discontinued, and access to sensitive information and sensitive information assets. Termination procedures should include use of a non-disclosure agreement to protect sensitive information, as well as the changing of encryption keys, passwords and access codes [6]. It is good practice for the licence holder or competent authority to recover and account for all official property (e.g. passes, including those for vehicles; uniforms; branded workwear).

2.9. A trustworthiness programme is intended to help identify precursory insider adversary behavioural patterns. An effective trustworthiness programme also focuses on identifying and addressing cultural or organizational factors that can reinforce such behaviour.

METHODOLOGIES FOR DETERMINING TRUSTWORTHINESS

2.10. The methodology used to determine the trustworthiness of individuals will vary depending on State laws, regulations or policies concerning personal privacy and job position. However, the methods used by licence holders or competent authorities for developing a trustworthiness programme will generally include the following elements:

(a) Establishing a policy for trustworthiness assessments using a graded approach according to the access and authority that the individual needs in relation to the facility and its assets. Access to sensitive information at the facility or while working remotely should also be considered.
(b) Developing objective criteria to form the basis for trustworthiness determinations.
(c) Identifying a range of aberrant behaviour that may demonstrate an increased risk of an insider becoming an insider adversary.
(d) Planning trustworthiness assessments for individuals both before and during employment which include the following activities:
    (i) Gathering information to determine whether an individual has exhibited any aberrant behaviour.
    (ii) Validating the information gathered.
    (iii) Assessing the information against established aberrant behaviour, making a trustworthiness determination for the individual through use of a decision making framework that allows information (e.g. criminal records, previous negative trustworthiness determinations) collected to be considered for its current relevance. For example, behaviour could be assessed on the basis of how long ago it arose, the seriousness of the issue or the age of the individual at the time that it occurred.
    (iv) Communicating and documenting an individual's trustworthiness determination.
    (v) If permitted by State laws, including a process by which an individual who has received a negative trustworthiness determination can appeal the result.

INTERFACES OF TRUSTWORTHINESS PROGRAMMES WITH NUCLEAR SECURITY CULTURE PROGRAMMES

2.11. Reference [5] defines the concepts, characteristics and indicators of a nuclear security culture while also providing a model of an effective nuclear security culture and describing the roles and responsibilities of institutions and individuals. IAEA Nuclear Security Series No. 28-T, Self-assessment of Nuclear Security Culture in Facilities and Activities [12], provides guidance on a comprehensive methodology for evaluating nuclear security culture in practice and IAEA Nuclear Security Series No. 38-T, Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and Other Radioactive Material [13], provides practical guidance on how to implement a systematic approach to enhancing nuclear security culture.

2.12. A robust nuclear security culture is an important element to counter insider and external threats. The overall objective of the nuclear security culture is to establish an organizational culture in which individuals willingly view nuclear security as their personal responsibility. Reference [5] defines 30 observable characteristics that can be used as indicators of an organization's nuclear security culture. Leadership behaviour that can foster effective nuclear security includes management oversight, well developed management systems that prioritize security, and an established behaviour observation programme to assess the trustworthiness of individuals on a continual basis. An example of personnel behaviour that can contribute to effective nuclear security includes professional conduct and adherence to procedures, performing tasks as assigned, handling of sensitive information and maintaining an awareness of potential safety concerns and security concerns.

2.13. The effectiveness of a trustworthiness programme is not only enhanced through initial and ongoing trustworthiness assessments of individuals, but it is also enhanced through the establishment of a robust nuclear security culture.

2.14. A strong nuclear security culture strengthens an individual's trustworthiness through a system in which peers and management respond appropriately to aberrant behaviour and reinforce behaviour that is consistent with security. Licence holders should have employment policies that promote and reward positive traits and desired behaviour such as equality and professional conduct while discouraging and penalizing inappropriate behaviour (e.g. harassment, bullying) in an effort to avoid individuals feeling marginalized, demotivated and potentially disaffected. Assistance programmes and reporting hotlines can help individuals to raise concerns, seek help and improve the nuclear security culture through direct or anonymous reporting.

INTERFACES WITH SAFETY PROGRAMMES

2.15. Human performance and human reliability are of vital importance in conducting safe, secure and effective nuclear operations. Safety programmes and human reliability programmes implement measures to monitor human performance and reliability, that can also be used in the context of a trustworthiness programme. For example, requirements for medical and psychological fitness for duty (e.g. testing for drug or alcohol abuse) of personnel are provided in IAEA Safety Standards Series No SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [14], and recommendations on establishing and implementing policies to address these requirements are provided in IAEA Safety Standards Series Nos SSG-75, Recruitment, Qualification and Training of Personnel for Nuclear Power Plants [15], and SSG-84, The Operating Organization and the Recruitment, Training and Qualification of Personnel for Research Reactors [16]. Reference [17] describes the assessment of competencies.

3. ROLES AND RESPONSIBILITIES WITHIN THE TRUSTWORTHINESS PROGRAMME

3.1. Roles within the trustworthiness programme include those of the State, designated competent authorities, licence holders, individuals and other stakeholders.

THE ROLE OF THE STATE

3.2. The State should establish trustworthiness programmes for nuclear security within the context of the State's legislative framework. A competent authority should be designated or established in State law to develop the regulatory requirements, to oversee the establishment and implementation of trustworthiness programmes for the State's nuclear security regime in order for the licence holders to grant access authorizations to nuclear material, other radioactive material, and sensitive information. The State should designate one or more competent authorities responsible for conducting, or regulating and overseeing trustworthiness assessments and determinations. Trustworthiness programmes can vary from one State to another. In some States, only one competent authority might be responsible for both trustworthiness assessments and determinations. In some States, the licence holder is responsible for trustworthiness assessments and determinations. A prerequisite is that the State, through it authorities, provides such necessary information on the individuals being assessed that is only available to the State. In the following text and in Figure 1, only the case where the designated competent authorities are conducting the assessments and determinations is described. However, the descripttion should be understood as covering assessments and determinations conducted by either competent authorities or licence holders.

3.3. The legal provisions of trustworthiness programmes for nuclear security should be consistent with national norms pertaining to the collection and use of personal information to ensure an equitable and sufficiently robust system for making a trustworthiness determination. Depending on the State's legal framework, specific provisions might be established for the collection of personal information and the conduct of trustworthiness assessments. Additionally, consideration should be given to establishing a legal requirement for cooperation and coordination with other competent authorities to allow compliance with a request for information required to make a trustworthiness determination. Laws also could be established to require that individuals disclose previously protected information. In such cases, legal precautions should be taken to ensure that such information is only used within the scope of the trustworthiness determination.

3.4. A State might already have an established trustworthiness programme that is not specific to its nuclear security regime. In this case, it might be considered more appropriate to utilize previously established and authorized trustworthiness determinations made by other competent authorities (e.g. intelligence, law enforcement) for nuclear programme employees.

3.5. A State can pass legislation or establish arrangements for the reciprocal recognition and communication of trustworthiness determinations between nuclear facilities and relevant government agencies, including competent authorities.

3.6. State provisions should exist to ensure the integrity and confidentiality of the assessment process and the outcome of trustworthiness determinations. Provisions of appropriate sanctions should be made, for example, to address any falsification of, misrepresentation of, or tampering with data or the process, either by the individual undergoing the trustworthiness assessment or by those responsible for the assessment or determination. Any falsified records, misrepresentation, or tampering with data or the process should be rectified and recorded for future reference, possible root cause analysis or identifying trends.

Enforcement of the trustworthiness programme

3.7. The State should establish sanctions to enforce the policies of the trustworthiness programme. Sanctions should be based on legal obligations, with the applicable offenses and penalties, concerning the implementation of the programme. The State's legal framework can include sanctions for employees for mishandling, misuse or unauthorized actions in relation to information. Sanctions could also address unauthorized actions undertaken by organizations (e.g. at the level of the State, competent authority, licence holder). Sanctions should be commensurate with the severity of the violation, and approved sanctions could include suspension with or without pay, downgrading the role of the employee, stripping access to and authority over sensitive information, employee reassignment or termination of employment. States can also pursue civil or criminal sanctions.

COMPETENT AUTHORITY RESPONSIBLE FOR OVERSEEING A TRUSTWORTHINESS PROGRAMME AND MAKING TRUSTWORTHINESS DETERMINATIONS

3.8. The State should designate a competent authority to perform the oversight of the trustworthiness programme, supported by the appropriate legal framework. The designated competent authority should develop regulations and guidelines for the trustworthiness programme, as well as oversight arrangements, data policies and licence holder procedures. The competent authority should ensure that the guidelines and procedures on trustworthiness are consistently implemented by the licence holder. This could be accomplished through an inspection programme (see para. 11.5).

3.9. Regulatory processes for trustworthiness assessments and determinations should document the following items:

(a) Description of the procedures to conduct pre-employment trustworthiness assessments and to make trustworthiness determinations;

(b) Description of the procedures to perform periodic trustworthiness assessments and make new trustworthiness determinations during employment including when changes are reported (e.g. those that are self-reported or reported by the licence holder);
(c) Identification of types and sources of information that can be used to conduct trustworthiness assessments;
(d) Application of criteria and processes to validate or possibly mitigate derogatory information, circumstances or actions;
(e) Verification of the qualifications and experience of those administering the processes;
(f) Confirmation of the period during which the determination will be considered valid;
(g) Management of personnel data using record keeping procedures to document completed trustworthiness assessments and determinations, including any documentation associated with appeals;
(h) Implementation of procedures to protect sensitive information gathered during the trustworthiness assessment;
(i) Application of provisions for the oversight of the trustworthiness programme;
(j) Description of frequency of trustworthiness assessments and description of procedures for updating records.

3.10. In some States, the competent authority responsible for oversight of the trustworthiness programme and the competent authority of the licence holder are two different competent authorities. However, in many States, the competent authority of the licence holder is the same as the competent authority responsible for oversight of the trustworthiness programme and is responsible for making a trustworthiness determination. The designated competent authority should follow regulations and guidelines established for the trustworthiness programme and established process for trustworthiness determinations. In addition, the designated competent authority should develop a notification process to communicate to the licence holder in a timely manner any relevant information regarding an individual's trustworthiness determination, which could include information on issues that might have arisen during the trustworthiness assessment. Licence holders should notify the competent authority that is making the trustworthiness determination of matters which come to its notice.

Responsibilities of personnel making a trustworthiness determination

3.11. A trustworthiness determination should be conducted by suitably qualified and experienced personnel and should be based on balanced judgement, of both the positive and negative aspects of the individual who is subject to the determination. The determination should be decided in a non-discriminatory manner, without personal prejudices, weighing the different factors and the security requirements of the job position in order to reach a conclusion on the individual's suitability to access nuclear material, other radioactive material or sensitive information.

3.12. Trustworthiness determinations should be based on all of the information provided, and if that information is insufficient, further enquiries should be undertaken.

3.13. The personnel responsible for trustworthiness determinations should be aware of their State's legal framework concerning the protection of privacy and measures to ensure information security, which includes how information is shared with external organizations and penalties for the misuse of information or not protecting information properly

3.14. The personnel responsible for trustworthiness determinations should not make a trustworthiness determination where there might be a conflict of interest in relation to the individual undergoing assessment. For example, they might know the individual in a personal capacity, or the person who is being assessed is responsible for their performance appraisal.

3.15. The personnel responsible for the trustworthiness determination are accountable for their decision relating to an individual made at a particular point in time, but it is the licence holder that will need to manage any subsequent issues that might arise.

COMPETENT AUTHORITY (OR LICENCE HOLDERS) RESPONSIBLE FOR TRUSTWORTHINESS ASSESSMENTS

3.16. The State could designate a competent authority responsible for conducting trustworthiness assessments. This competent authority should follow regulations and guidelines established for the trustworthiness programme and established process for gathering information. The competent authority conducting the trustworthiness assessment may need to rely on other competent authorities within a State to supply personal information about the individual undergoing the trustworthiness assessment. This information could include, for example, criminal records, financial data, previous national residency data or historical record of professional conduct. Depending on the type of information needed for the trustworthiness assessment (see Section 4), more than one competent authority could be responsible for submitting information. Competent authorities should establish processes to preserve data privacy, information integrity and to transmit information in a secure and lawful manner.

Gathering information for trustworthiness assessments

3.17. States should consider establishing regulations that identify other competent authorities (e.g. intelligence, law enforcement), third parties (e.g. lending institutions, previous employers, universities) and persons (e.g. relatives, friends, business associates) who can be approached to provide information on the individual undergoing assessment. The trustworthiness assessment process generally includes consent, through physical or digital signature, from the individual under assessment.

3.18. While the information provided by other competent authorities, third parties and persons should generally be considered as accurate, mistakes can nevertheless be made. Any discrepancy when

comparing information provided should be verified in all cases before the trustworthiness determination is made. Such verifications should also be performed in the case of a negative trustworthiness determination, before the individual is notified.

3.19. The competent authority should request information to be submitted in a timely manner, and should ensure that any sensitive personal information is received through a secure medium. Delays in receiving relevant information could delay employment decisions or lead the licence holder to implement expensive measures (e.g. escorting) until such time as the trustworthiness determination is completed. Therefore, the optimization of resources should be undertaken to avoid unnecessary delays in trustworthiness determinations.

LICENCE HOLDERS

3.20. Licence holders should be required to implement trustworthiness programmes as part of their licensing or other regulatory requirements. Licence holders should maintain up-to-date records of trustworthiness determinations for all of their employees, contractors and vendors, in accordance with national requirements.

3.21. The licence holder should develop a list of the job positions subject to a trustworthiness determination using the graded approach and based on a job task analysis (see para. 4.7). The list should be approved by the competent authority for the licence holder. Individuals seeking a position with the licence holder should be informed of the trustworthiness assessment and determination process when they are submitting an application for employment.

3.22. Licence holders should ensure that individuals subject to a trustworthiness determination are aware of the responsibilities of being in the trustworthiness programme, including reporting any aberrant behaviour observed in others or on any changes in their own personal circumstances.

3.23. Licence holders should have documented procedures for reporting data from the trustworthiness programme to the designated competent authority.

3.24. Licence holders should follow the procedures approved by the competent authority for collecting information (e.g. identity documentation, work visa) from an individual during pre-employment before seeking a trustworthiness determination.

3.25. The licence holder should maintain an effective working relationship with other competent authorities (e.g. the competent authority responsible for trustworthiness programmes, intelligence, law enforcement) as well as local law enforcement in accordance with State laws, regulations and policies.

3.26. While awaiting a trustworthiness determination for an individual, if a licence holder identifies aberrant behaviour being exhibited by an individual, the behaviour should be reported to the competent authority making the trustworthiness determination. The licence holder should nevertheless proceed

with any disciplinary actions and not wait for the determination from the competent authority. Trustworthiness determinations and performance management are separate processes, and thus licence holders should not use trustworthiness determinations as a substitute for disciplinary action.

INDIVIDUALS SUBJECT TO TRUSTWORTHINESS DETERMINATIONS

3.27. Individuals subject to trustworthiness determinations should report the required personal information accurately and honestly, both during the pre-employment and employment periods.

OTHER STAKEHOLDERS

3.28. Other organizations may have individuals whose work duties fall within the framework of a State's nuclear security regime that could also be subject to a trustworthiness determination by their respective competent authority. For example, law enforcement, customs officials and border security who are involved in systems and measures to detect and respond to material out of regulatory control can be subject to a trustworthiness programme by their competent authority. In this case, the relevant competent authorities should coordinate with each other to establish procedures to share information in relation to trustworthiness determinations.

3.29. Many States rely on personnel from organizations such as universities to provide scientific support to law enforcement agencies responding to incidents involving nuclear or other radioactive material out of regulatory control. In such cases, the State should consider having the personnel involved obtain a positive trustworthiness determination before being eligible to provide such support.

ACTIONS IN THE TRUSTWORTHINESS PROCESS

3.30. The trustworthiness assessment and determination process is initiated when an individual needs access to nuclear material, other radioactive material or sensitive information. In order for the licence holder to grant access, the trustworthiness for the individual needs to be determined. Figure 1 illustrates the actions that the licence holder and competent authorities take in the trustworthiness assessment and determination process in order to grant access to an individual.

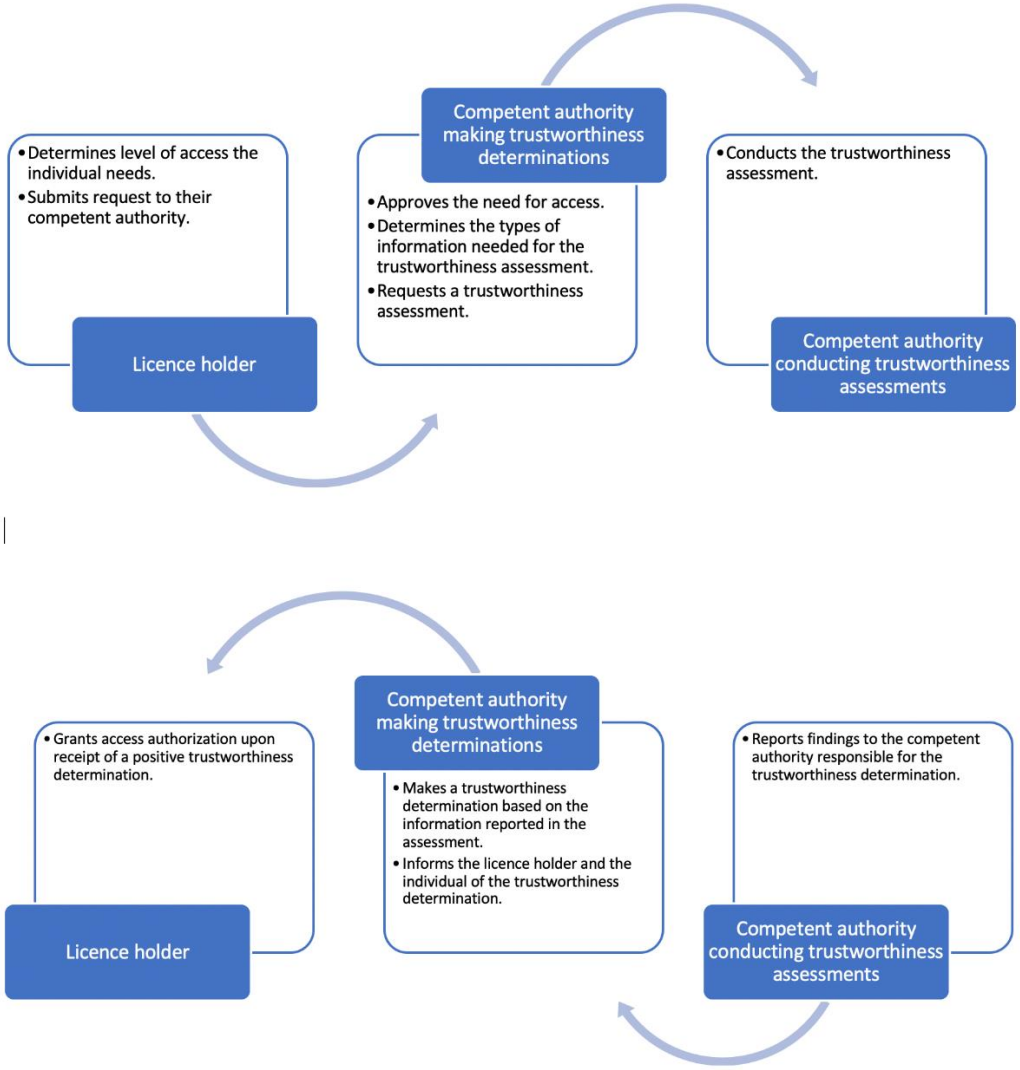

FIG.1. Actions of the licence holder and competent authorities in the trustworthiness process.

4. IMPLEMENTATION OF TRUSTWORTHINESS PROGRAMMES USING A GRADED APPROACH

4.1. The designated competent authority should develop trustworthiness determination criteria to ensure a consistently applied and effective trustworthiness programme. These criteria should consider risk reduction, cost effectiveness and State laws for privacy as it relates to those subject to a trustworthiness determination.

4.2. The State can establish effective and consistent requirements for trustworthiness determinations using the risk management objectives (e.g. unauthorized removal or potential consequences of sabotage) of the nuclear security programme. [18].

4.3. Implementing all the elements of a trustworthiness programme for all individuals involved in the nuclear programme could be challenging both in terms of cost and human resources. For this reason, a graded approach should be followed in the implementation of trustworthiness assessments.

4.4. As part of a graded approach, different types of information should be collected for the trustworthiness assessment on the basis of the attractiveness and category of the nuclear material, the category of other radioactive material and the class of sensitive information. Information that could be collected includes the following:

(a) Identity verification (including dual nationality status);
(b) Relevant personal and professional history, which could include details concerning family members, friends and colleagues;
(c) Travel history;
(d) Education and previous employment verification;
(e) Financial evaluation;
(f) Character evaluation;
(g) Criminal history review;
(h) Drug and alcohol testing;
(i) Medical information relevant to performing job functions;
(j) Psychological assessment from a certified credentialed psychologist, for the most critical positions;
(k) Polygraph testing, for the most critical positions.

4.5. Table 1 is an example of the trustworthiness assessment information that could be used to assess the trustworthiness of an individual for access to each category of nuclear material, other radioactive material, vital areas, and class of sensitive information. The trustworthiness assessment criteria should be commensurate with the access authorization needed and the potential consequences of a malicious act. The trustworthiness assessment criteria were developed using the categorization tables for nuclear material and other radioactive material and the classification framework for sensitive information provided in table 1 in Ref. [1], table 7 in Ref. [19], and annex I to Ref. [11], respectively.

TABLE 1. A GRADED APPROACH FOR TRUSTWORTHINESS ASSESSMENTS

	Trustworthiness assessment area			
	Category of nuclear material or other radioactive material and class of information			
Type of information collected ↓	Quantities less than Category III, natural uranium, depleted uranium and thorium, Radioactive Sources Category 4, 5	Nuclear Material Category III, Radioactive Sources Category 1, 2, 3 Restricted Information	Nuclear Material Category II, Vital Areas, Confidential Information	Nuclear Material Category I, Vital Areas, Secret Information
Identity verification	x	x	x	x
Employment verification	x	x	x	x
Education verification	x	x	x	x
Personal history		x	x	x
Financial evaluation		x	x	x
Criminal history		x	x	x
Character evaluation			x	x
Drug and alcohol testing			x	x
Medical evaluation			x	x
Psychological assessment				x
Polygraph testing				x

4.6. Trustworthiness assessments for individuals at a nuclear facility with access to the protected area, vital area, inner area or hardened room should be more frequent and comprehensive than trustworthiness assessments for individuals that need access to the limited access area. Individuals that participate in critical activities, such as the transport of nuclear material, should also receive trustworthiness assessments. Figure 2 illustrates a typical layout at a nuclear facility. In such a facility, for example, the trustworthiness assessment for an individual who needs authorized access to the hardened room or enclosure (blue) will be more comprehensive than the trustworthiness assessment for an individual who needs authorized access to the inner area (pink) or the vital area (purple). The trustworthiness assessment for individuals who need authorized access to the inner area and the vital area will be more comprehensive than the trustworthiness assessment for individuals who need access to the protected area (orange). All of the above areas will involve more comprehensive assessments than the assessment undertaken for the limited access area (yellow).

4.7. Once a facility has designed the protection system of its nuclear material and related information and equipment, areas and systems, following a graded approach, a job task analysis will determine which job positions need direct access to secure areas and which ones can be separated out to the less secure areas. The facility management can then begin to select a minimal number of individuals who

will have direct and unescorted or unsupervised access to nuclear material, other radioative material, sensitive information, equipment and systems. These are the individuals for which the most rigorous trustworthiness assessments should apply. The relevant job positions might include nuclear material handlers, central alarm station operators, alarm technicians, reactor operators and engineers, maintenance engineers and technicians, personnel conducting vulnerability assessments, research scientists, information technology and operational technology experts, individuals involved in the transport of nuclear material. Depending on State laws, the individuals in these job positions would likely be subject to ongoing trustworthiness assessments, drug and alcohol testing and psychological personality profiling evaluations.

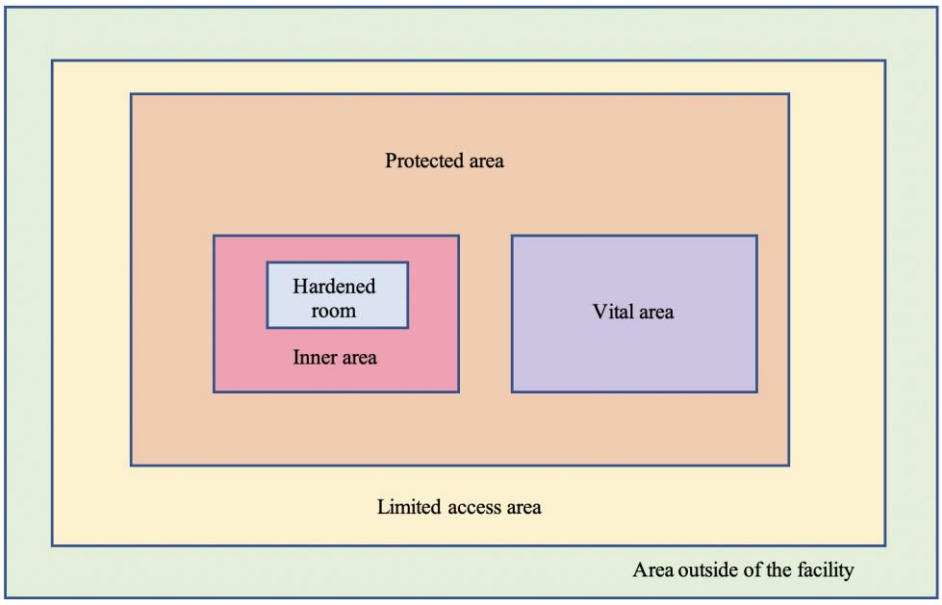

FIG.2. Nuclear facility layout (adapted from Fig. 7 of Ref. [18]).

TRUSTWORTHINESS ASSESSMENTS FOR OTHERS

4.8. Trustworthiness assessments should not be limited to employees of the licence holder (physically present at the facility or working remotely). Assessments can also be extended to foreign personnel, temporary personnel, students and interns, supply chain employees, and visitors to the facility.

Foreign personnel

4.9. Foreign nationals support many areas of research and education and might need access to nuclear material, other radioactive material or to sensitive information, including those that can be accessed remotely to conduct assigned duties. Host States could establish agreements (e.g. memoranda of understanding) with other States or international organizations to receive information on the personal background and employment history of foreign nationals to assist the trustworthiness determination process. Information provided by other States or international organizations should be verified to the

extent possible. If personal information cannot be obtained from the State in question, then access authorization or employment could be restricted or denied. If State laws permit, then access could be granted under a special decision by the competent authority.

4.10. The policies of a State will determine whether arrangements allow for trustworthiness assessments to be performed on foreign nationals. Where they do, States should be mindful that if residency is limited, there could be an insufficient presence in that State for there to be sufficient information in order to make a trustworthiness determination. The provision of foreign police certificates could provide additional assurance in the trustworthiness of the individual; as could the validation of a trustworthiness determination in the individual's home State, where verification arrangements exist. States should ensure that foreign personnel have the right to work in the host State and that trustworthiness determinations do not extend beyond the expiry of the work permit. Any behavioural indicators suggesting divided loyalty should lead to an additional trustworthiness assessment.

Temporary personnel

4.11. Paragraph 4.20 of Ref. [6] states:

> "Persons whose trustworthiness has not been determined or whose duties do not require a trustworthiness assessment (e.g. temporary repair staff, administrative staff, maintenance staff, construction workers, visitors) should be escorted into [limited access areas, protected areas], vital areas or inner areas [or hardened rooms or enclosures] by persons who have authorized access and are not required to be themselves escorted."

4.12. A graded approach should be applied for trustworthiness assessments that involve escorted access of temporary workers. Depending on State laws and limitations (e.g. time, cost, human resources), trustworthiness assessments for temporary workers could be limited to verification of employment and identity, and criminal records.

4.13. Temporary workers who need access to nuclear material, other radioactive material or sensitive information should undergo a trustworthiness assessment based on a graded approach (see Table 1) to be granted an access authorization to perform their duties. These duties could include technical support activities, such as nuclear facility design, calibration and maintenance, operational and security functions, or computer security support functions. When the financial costs and time needed to make a trustworthiness determination associated with granting temporary access are high, escorted access should be considered.

4.14. When the temporary worker belongs to an external organization, appropriate arrangements should be made by the licence holder to liaise with the external organization to ensure that the

appropriate trustworthiness determination is transferred and that concerns are properly communicated to the licence holder.

4.15. The licence holder should ensure that temporary workers are treated in an equivalent manner to permanent personnel, although employment rights may differ. Given the transient nature of such temporary positions, arrangements to deny the access of temporary workers to the premises of the licence holder, or to sensitive information when working remotely, should be made in real time, either when the temporary worker leaves the licence holder or when the contract ends.

4.16. The nuclear security culture should encourage personnel, contractors and temporary workers to feel equal responsibility for reporting concerns relating to trustworthiness of inviduals, despite the difference in employment status, and even in cases where it would mean reporting on another individual. To maximize the likelihood of reporting, a reporting hotline should be made available to all personnel, whether temporary or permanent.

Students and interns

4.17. Depending on State laws and limitations (e.g. time, cost, human resources), trustworthiness assessments for students and interns could be limited to a verification of identity, nationality and the educational institution. Owing to this, students and interns whose trustworthiness has not been determined should be escorted at all times when needing access to an area that requires a trustworthiness determination.

Supply chain employees

4.18. A large number of external organizations can be involved in the supply chain, either from other regions of the State or from other States. The globalization of the supply chain presents a number of challenges for the State's competent authorities and licence holders.

4.19. Personnel in the supply chain should feel equal responsibility for reporting aberrant behaviour or concerns relating to the trustworthiness of individals, even those that necessitate reporting other personnel, contractors and temporary workers. To maximize the likelihood of reporting, any reporting hotline should also be made available to personnel in the supply chain.

4.20. Given the transient nature of supply chain employment at facilities, arrangements to deny access to the premises of the licence holder or to sensitive information should be made in real time, either when the employee in the supply chain leaves his or her organization or when the facility's contract with the supply chain organization ends.

Information security

4.21. Individuals in the supply chain may have access to potentially sensitive information, including information on the design necessary for the production of specified items that are being procured by the licence holder.

4.22. Individuals within the supply chain who have access to sensitive information should be subject to the same level of trustworthiness assessment as the staff of the licence holder.

4.23. Contractual agreements can be established between States to extend the trustworthiness programme of the licence holder to the personnel of a supply chain organization from another State. These agreements would enable the competent authority for the licence holder to establish the requirements of the trustworthiness programme for organizations within the supply chain.

Counterfeit, fraudulent or suspect items

4.24. The increasing occurrence of counterfeit, fraudulent and suspect items arising within the global supply chain, including within the nuclear supply chain, is a cause for concern. These items often do not undergo the same rigorous quality control procedures as legitimate items, and can deviate from prescribed specifications. Within the nuclear supply chain, counterfeit, fraudulent and suspect items can diminish the integrity of equipment, systems, structures, components or devices that contribute to nuclear safety and nuclear security.

4.25. The production and insertion of counterfeit and fraudulent items into the supply chain can be considered a criminal or other intentional malicious act, which can be perpetrated by entire companies or by individuals employed within the supply chain. The extension of a trustworthiness programme to organizations within the supply chain can thus assist such organizations in identifying individuals who are likely to participate in such malicious acts.

4.26. Procedures should be implemented to determine the likelihood that a supply chain organization would willingly participate in the production and insertion of counterfeit, fraudulent and suspect items into the supply chain. Additional information on mitigating counterfeit, fraudulent and suspect items can be found in Refs [20] and [21].

4.27. The actions taken by supply chain organizations to comply with the requirements of the trustworthiness programme will contribute to enhancing the protection of sensitive information; mitigating counterfeit, fraudulent and suspect items; and increasing overall transparency and trust between the licence holder and the entities within the supply chain that are engaged in a business relationship.

Visitors

4.28. Depending on State laws and limitations (e.g. time, cost, human resources), trustworthiness assessments could be limited to a verification of identity and nationality. Owing to this, visitors whose trustworthiness has not been determined should be escorted at all times when needing access to an area that requires a trustworthiness determination.

4.29. States should consider the length of time needed to conduct a trustworthiness assessment for authorized access when they define visitors as short or long term, for instance short term (i.e. when a

trustworthiness assessment is unlikely) or long term (i.e. when a trustworthiness assessment should be completed based on a graded approach). The identity of all visitors should be verified regardless of the duration of the visit, as should the person's right to be present in the State in the case of a foreign national.

4.30. The usual control measures such as searches for recording devices or cameras, escorting and reporting of aberrant behaviour should remain routine.

4.31. Where a visitor will be subject to a trustworthiness determination, a statement that such an assessment will be performed should be included in the visitor request forms that are completed by the individual.

5. ESTABLISHING CRITERIA FOR CONDUCTING TRUSTWORTHINESS ASSESSMENTS AND MAKING TRUSTWORTHINESS DETERMINATIONS

5.1. The frequency of trustworthiness assessments will often differ from one State to another since these assessments will depend on national legislation; the regulatory approach used; financial impact; the type of nuclear facility; the category of nuclear material and the category of the radioactive material; the associated facilities and activities; risk assessments and the consequences of potential malicious acts. The competent authority should define the minimal period between the trustwothiness determinations. The following have been identified as possible opportunities for the conduct of trustworthiness assessments:

(a) During pre-employment periods;
(b) Periodically during employment, including when there is a change in status or circumstances (e.g. new partner, new co-residents, conviction, debt, illness, trauma, extended absence, disciplinary proceedings, other significant life stressors);
(c) Occurrence of an incident that was defined on the basis of established criteria (e.g. inappropriate social media posting, suspicious approach from a third party, disciplinary action, positive test for alcohol or unlawful substances).
(d) At the time of a change in position, which involves a more stringent trustworthiness assessment;
(e) At the expiry date of a validity period for a trustworthiness determination.

DATA PRIVACY CONSIDERATIONS FOR TRUSTWORTHINESS ASSESSMENTS

5.2. The collection and analysis of information in the context of trustworthiness assessments should be conducted in compliance with the State's legislation concerning the protection of privacy. Information from trustworthiness assessments should be considered sensitive information, as this information could be used for blackmail or extortion. Most national privacy regulations should therefore mandate the protection of this type of information [11]. Data should be protected in compliance with

State laws. Legal, technical and administrative measures should be established and implemented to minimize intrusion into personal privacy and to maximize the protection of data, with the rules of the assessment process being made fully transparent and the individuals being informed of their rights regarding the protection of privacy and measures for information security. Such legal, technical and administrative measures should also address information sharing within the assessment process to facilitate decision making for trustworthiness determinations while also respecting individual privacy.

5.3. Measures addressing information security should be implemented using a risk informed approach at all stages of the trustworthiness assessment process, for instance during the collection, analysis, storage, retrieval, processing and destruction of information. Any access to documentation concerning trustworthiness assessments and determinations should be granted on a 'need to know' basis to authorized individuals so that they are able to perform their assigned duties. States can assign classification levels to certain types of information in accordance with the guidance provided in Ref. [19].

BEHAVIOURAL INDICATORS OF INSIDER ADVERSARIES

5.4. Certain aberrant behaviour could indicate that an individual is predisposed to commit a malicious act. While not all behaviour will necessitate formal action, in combination with other factors, or when the consequences are significant and left unresolved, such behaviour could pose a risk to an individual's well-being, to the security arrangements of an organization or to the State's national security.

Aberrant behaviour

5.5. Certain aberrant behaviour could render an individual vulnerable to exploitation, and could ultimately compromise an organization's security arrangements. The indicators listed below are more common than those associated with insider adversary activity, but could indicate an increased potential towards malicious acts. Individuals experiencing stressful situations can sometimes exhibit aberrant behaviour that could result in a security concern. Where some doubt exists in relation to an individual's ongoing suitability to hold a positive trustworthiness determination, early intervention is key to rapid and effective resolution. Examples of aberrant behaviour could include the following:

(a) Use of illegal drugs, abuse of legal drugs or alcohol;
(b) Unwillingness to comply with rules, policies or procedures;
(c) Repeated irresponsibility in performing assigned duties;
(d) Disregard for authority or difficulty accepting feedback or criticism;
(e) Financial problems linked to gambling or financial irresponsibility;
(f) Indications of deceit, delinquent behaviour or lack of dependability;

(g) Symptoms of a mental or physical condition that impairs performance or adversely affects judgement;
(h) Behaviour that warrants criminal investigation, or results in arrest or conviction;
(i) Physical aggression and attempted or threatened destruction of property or life;
(j) Inability to deal with stress, or the appearance of being under unusual stress;
(k) Verbal hostility, aggression towards authority or fellow workers, making malicious statements about fellow workers and uncontrolled anger;
(l) Significant changes in behaviour (e.g. moodiness, loss of inhibition, social disengagement);
(m) Dissatisfaction with the employer or competent authority.

POTENTIAL INSIDER ADVERSARY INDICATORS

5.6. If an individual exhibits one or more of the potential insider adversary indicators listed below, it could be cause for concern and merit further investigation. Insider adversary indicators could include the following:

(a) Unexplained affluence;
(b) Unreported conflicts of interest;
(c) Failure to report foreign travel;
(d) Unusual interest in information outside the current job scope;
(e) Unusual work hours;
(f) Unreported or concealed contacts with foreign nationals (e.g. requests for illegal or unauthorized access to classified or sensitive information, or to digital assets);
(g) Unreported contacts with foreign governments, military or intelligence officials;
(h) Attempts to gain access to sensitive information or sensitive information assets without the 'need to know' or authorization;
(i) Unauthorized removal or sabotage of nuclear or other radioactive material, sensitive information or digital assets from authorized locations without authorization;
(j) Attempts to gain access to any areas for which access authorization has not been granted;
(k) Association or sympathy with criminal or terrorist individuals or groups;
(l) Behaviour involving questionable judgment, integrity or organizational and national loyalties;
(m) Uncharacteristic changes in appearance or behaviour;
(n) Failure to disclose relevant medical conditions;
(o) Unexplained absences.

ORGANIZATIONAL FACTORS ASSOCIATED WITH INSIDER ADVERSARIES

5.7. In some cases, organizational factors can develop over time and weaken the reliability, integrity or honesty of individuals. These organizational factors cannot be associated with personal circumstances but rather are a result of mismanagement. Some examples of organizational factors that can contribute to a deterioration in the reliability, integrity and honesty of individuals over time include the following:

(a) Poor communication by managers, which invokes feelings of injustice;
(b) Favouritism (e.g. rewarding or promoting less qualified individuals);
(c) Lack of recognition by management of superior efforts;
(d) Poor treatment of the individual (e.g. harassment, lack of respect, hostile work environment);
(e) Absence of, or lack of focus on, sustaining a nuclear security culture.

5.8. Licence holders should ensure that employment policies and contracts, including those in relation to the supply chain, support an environment that does not tolerate discrimination or unsatisfactory behaviour. Appropriate avenues should also exist to raise concerns in order to reduce the possibility of individuals becoming disgruntled or disaffected as a result of unacceptable practices, or as a result of such practices not being properly addressed.

6. PROCESSES FOR THE IMPLEMENTATION OF A TRUSTWORTHINESS PROGRAMME

6.1. The trustworthiness programme should be implemented at various levels, including that of the State, competent authority and licence holder, as well as at the level of other organizations supporting the functions of the licence holder (e.g. contractors, vendors). The steps for implementing a trustworthiness programme are nevertheless the same for each level. Trustworthiness programmes developed for other security areas of the State can be used in whole or in part for nuclear security. Alternatively, specific nuclear security trustworthiness programmes can be developed. Where a trustworthiness programme for nuclear security is built on existing State or industry programmes designed for other purposes, the competent authority should ensure that the objectives relating to nuclear security trustworthiness are consistent with and adequately incorporated to the objectives of the existing programmes. The steps to be taken to establish a trustworthiness programme are the following:

(1) Designation of a competent authority;
(2) Identification of stakeholders and a method of collaboration;
(3) Development of governance and policy documents;
(4) Implementation of training and awareness programmes;
(5) Conduct of trustworthiness assessments;
(6) Evaluation of the trustworthiness programme.

Designation of a competent authority

6.2. The first step in implementing a trustworthiness programme is for the State to designate the competent authority responsible for developing and implementing the programme. The designated competent authority should be familiar with relevant legislative and regulatory provisions and the role of a trustworthiness programme for nuclear security.

Identification of stakeholders and a method of collaboration

6.3. The implementation of an effective trustworthiness programme could involve collaboration by the competent authority with multiple stakeholders, including those who develop, manage, implement and are subject to the programme. Stakeholders can also include organizations with legal, medical, psychological and regulatory expertise, which can provide advice to the competent authority on ways to ensure that the programme meets the relevant requirements. Collaborative development of the programme with input from all these stakeholders provides mechanisms to identify issues or concerns early in the development process and supports the development of an effective and sustainable programme that meets all needs of all stakeholders.

Development of governance and policy documents

6.4. The State should provide guidance to the competent authority on trustworthiness programmes, including on privacy, and the appropriate levels of transparency and effectiveness of the programmes. This guidance should be established on the basis of legislative provisions and regulations. It should outline clear lines of authority and responsibility, and describe the programme at a sufficient level of detail to ensure consistent implementation. The guidance should also identify oversight organizations; programme goals; organizations, activities and job positions subject to the trustworthiness programme; mechanisms by which individuals are assessed; and the process to appeal a negative trustworthiness determination, if applicable. In accordance with State laws, guidance should also clearly communicate to those subject to a trustworthiness determination the requirements for their position; information that will be gathered about individuals; the ways in which the information will be used, shared and stored; the obligations and rights of individuals with respect to the assessment process; and any arrangements to appeal a negative trustworthiness determination, if applicable.

Implementation of training and awareness programmes

6.5. The competent authority responsible for conducting the trustworthiness assessment and the competent authority responsible for making trustworthiness determinations should receive training on how to conduct their tasks in accordance with the policies and procedures of the trustworthiness programme. The overall objective of the training programme is to ensure that the individuals responsible for trustworthiness assessments and determinations are suitably qualified.

6.6. Competent authorities should require licence holders to raise awareness on the role that the trustworthiness programme has in the overall nuclear security culture, for instance through a nuclear security awareness programme [6]. Individuals who are subject to trustworthiness assessments should be aware of their roles, the ways in which they can contribute to the process, and the reasons why the programme is important for nuclear security (see paras 4.32–4.33 of Ref. [6]). Training and awareness programmes should be conducted on a regular basis to enhance commitment to the nuclear security culture.

Conduct of trustworthiness assessments

6.7. Once guidance for the trustworthiness programme is established, and training and awareness activities are completed, the competent authority can initiate trustworthiness assessments.

Evaluation of the trustworthiness programme

6.8. Once a trustworthiness programme is implemented, competent authorities should periodically evaluate the programme. Evaluation of the programme should include audits and inspections of the trustworthiness programme, and where applicable, feedback from the licence holder regarding the effectiveness of the programme. The results of the evaluation should be used to identify trends regarding trustworthiness related issues and for programme improvement. Audits and inspections of the trustwothiness programme are described in Section 11.

PROCESS FOR CONDUCTING TRUSTWORTHINESS ASSESSMENTS

6.9. Trustworthiness assessments can vary but generally the following steps can be identified in the process for conducting trustworthiness assessments:

(1) Determination of the access needed for the individual;
(2) Submission of a request for a trustworthiness assessment;
(3) Collection of information;
(4) Validation of information and collection of additional information;
(5) Determination of trustworthiness;
(6) Documentation and communication of the trustworthiness determination;
(7) Management of appeals.

Determination of the access needed for the individual

6.10. The licence holder determines the level of access needed (e.g. limited access area, protected area, inner area, vital area, type and class of sensitive information) for the individual on the basis of the individual's job functions and whether the position entails the individual working alone. Access level

can vary depending on the type of facility. The need for access should be confirmed by the manager or supervisor.

Submission of a request for a trustworthiness assessment

6.11. Once the access needed is determined, the licence holder then submits a formal request to their competent authority to initiate the trustworthiness assessment. This request should be documented with the appropriate justification.

Collection of information

6.12. The competent authority responsible for trustworthiness determinations approves the assessment request and determines the type of information needed to make a trustworthiness determination (see paras 6.17 and 6.18). The competent authority then requests the competent authority responsible for trustwortiness assessments to initiate the process of collecting and validating the information ensuring that the information requests are in accordance with State laws, regulations and policies. In some cases, individuals might be requested to waive specific privacy rights so as to allow access to information that is necessary to conduct the assessment. These requests should be clearly communicated to the individual and should be considered only when necessary.

Validation of information and collection of additional information

6.13. After the information is collected, the competent authority responsible for the assessment should validate the information provided. Standards for what constitutes sufficient validation and methods to validate information should be documented in the procedures for trustworthiness assessments. For more comprehensive trustworthiness assessments, independent forms of validation from different organizations (e.g. government agencies, universities, financial institutions) could be needed for key pieces of information. During this comprehensive validation, the competent authority conducting the assessment should also gather any additional information needed to assess the individual against established criteria. Procedures should be defined to establish methods for collection of information, ensuring that such methods adhere to State laws, regulations and policies. Personnel who are responsible for gathering information should be suitably qualified and experienced. Records of all information gathering activities should be retained for audit purposes (see Section 11). A reporting process should also be established to allow individuals the opportunity to report inappropriate conduct by the personnel gathering or validating the information during the information gathering process.

Determination of trustworthiness

6.14. After the information has been gathered, the competent authority responsible for the trustworthiness determination then assesses the information using an established methodology to determine whether the individual is suitable for a positive trustworthiness determination. Personnel responsible for performing trustworthiness determinations should be suitably qualified and experienced

in applying the methodology, and in evaluating both aggravating and mitigating factors in a balanced manner so as to ensure that determinations are performed consistently. Oversight of the personnel designated to make trustworthiness determinations should be established so as to ensure that one person is not solely responsible for trustworthiness determinations.

Documentation and communication of the trustworthiness determination

6.15. Trustworthiness determinations should be documented and communicated to the licence holder who requested the determination. The trustworthiness determination should be communicated through secure and verifiable communications methods. Records of the trustworthiness determination, and justification for the corresponding access authorization, are to be retained for potential audit of the evaluation process and for oversight purposes.

Management of appeals

6.16. Trustworthiness assessment processes could also include an appeal process, if permitted under State legislation, allowing individuals to appeal a negative trustworthiness determination. Documentation should be made available on the appeal process, and should include information on what is considered acceptable grounds for appeal; the basis on which a trustworthiness determination can be reversed; designation of the authority granting or denying the appeal; the period within which the request to hear an appeal should be made; how the final determination is recorded and communicated; and whether any additional avenue of appeal exists (see paras 9.4–9.7 for more information on the appeal process).

SOURCES OF INFORMATION FOR A TRUSTWORTHINESS ASSESSMENT

6.17. Trustworthiness assessments involve the collection and review of personal information to justify the access authorization requested. The type of information used in the assessment should be determined by the competent authority and limited to only information that is necessary to evaluate an individual's trustworthiness using established methodology. This information should be gathered in accordance with State laws and the protection of privacy.

6.18. Sources of information used in the assessment may include the following:

(a) Self-reported information and information reported by others: This can be obtained in written form (e.g. answers to a questionnaire). Interviews can also be used to resolve information gaps. Information gathered through questionnaires or interviews should be verified by independent sources, where possible. In addition, the identity of any person who provides information concerning an individual who is undergoing a trustworthiness assessment should be verified independently.

(b) Identity documents: Acceptable documents for the verification of an individual's identity include identification documents issued by the government or by other trusted organizations. Any information that positively verifies the identity of the individual being assessed is an essential element in the trustworthiness assessment process.

(c) Personal record checks: These could consist of the verification of employment records, educational records, criminal history, or financial records. It might also include verification of other available information sources that relate to the established trustworthiness criteria.

(d) Physical examination records: Physical examination could include drug and alcohol testing, medical evaluation, psychological assessment, or polygraph testing.

(e) Publicly available information: This information could also be consulted, for example news articles, technical or scientific publications or presentations, self-published material, images, recordings, social media posts and artificial intelligence platforms.

(f) Information regarding abnormal activity in facility computer systems (e.g. physical protection systems, closed-caption television, nuclear material accounting and control systems).

FREQUENCY OF TRUSTWORTHINESS ASSESSMENTS

6.19. Trustworthiness assessments can be performed once, or they can be periodic, ongoing or incident based. The frequency of trustworthiness assessments should be determined by the competent authority using a graded approach on the basis of the individual's role and previous trustworthiness determinations.

6.20. Trustworthiness assessments are normally conducted once for individuals with temporary access or with limited access to nuclear material, other radioactive material or sensitive information.

6.21. Periodic trustworthiness assessments can be conducted at set intervals in time (e.g. every five years). The frequency of periodic assessments should be decided by the State or the competent authority. Periodic trustworthiness assessments could, for example, reveal relationships that are susceptible to collusion (e.g. marriage between individuals with the same access authorization) or identify emerging factors (e.g. financial difficulties) that could serve as a source of coercion. For individuals with long term access to nuclear material, other radioactive material or sensitive information, periodic assessments are considered more appropriate to assess whether the personal circumstances of an individual have changed and could potentially alter the initial trustworthiness determination.

6.22. Incident based trustworthiness assessments can be initiated on the basis of the results of reporting programmes or of relevant incidents. Such incidents could include self-reported status changes (e.g. criminal offences, serious financial issues, disciplinary actions, relevant psychological or other illnesses), security incidents or other criteria. The criteria to initiate a reassessment as the result of an incident should be documented by the competent authority as part of the procedures for the

trustworthiness programme so as to ensure consistency and transparency when implementing the reassessment.

7. MAINTAINING RECORDS FOR A TRUSTWORTHINESS PROGRAMME

TYPE OF DOCUMENTATION

7.1. The trustworthiness assessment process involves multiple types of documentation in paper or electronic format, such as the following:

(a) Requests, including justifications, by the licence holder for trustworthiness assessments;
(b) Information provided by the individual undergoing the assessment in the form of answers to questions and verification documents;
(c) Information, verification documents and database queries or reports provided by third parties;
(d) The trustworthiness determination, including information concerning the justification for the trustworthiness determination by the competent authority;
(e) The basis for, and results of, any subsequent administrative actions (see para. 7.11).

7.2. This documentation contains personal information, which should be the subject of information security measures and made available on a strict need to know basis. Information security measures protect the privacy of the individual and ensure that the individual is not exposed to future attempts at coercion. Information should be shared only on a need to know basis, for each type of documentation, in an effort to ensure that those initiating and conducting the assessments only have access to the information that is necessary to perform their assessment functions. Individuals who have access to view, create or modify documentation concerning trustworthiness assessments should have previously undergone a trustworthiness assessment at the appropriate level, as determined by the State. When documentation concerning trustworthiness assessments are created or modified, they should be a verified by a second person who is suitably qualified and has undergone a trustworthiness assessment at the appropriate level.

7.3. States should ensure that the processes associated with trustworthiness assessments are accompanied by a privacy statement indicating how personal information will be processed. This privacy statement should include the procedure to be followed in the case of a breach of these arrangements. Some States also have an official body to which breaches can be reported.

7.4. Persons who manage or handle personal information should be appropriately trained and aware of the consequences of breaching the privacy statement, since it could potentially undermine the willingness of individuals to disclose information relevant to the assessment, and have reputational implications for the overall process and the licence holder.

RECORD KEEPING

7.5. Policies for record keeping should be established to ensure records are retained in order for the competent authority to undertake audits of trustworthiness determinations (see Section 11). The need to preserve records for programme and evaluation purposes should be balanced against concerns of retaining large amounts of sensitive personal information. Personal information should be maintained for the period approved by the competent authority. Information on trustworthiness determinations and justification for granting or revoking access authorization should be retained for the duration of the trustworthiness determination. Such information can also be maintained for a set period after the anticipated end of employment, or for longer periods where national security concerns have been identified. Evaluations should be used to ensure that policies and procedures are correctly followed in terms of record keeping, storage and disposal.

7.6. Policies for record disposal should be establishd to ensure that any documentation that is no longer needed is disposed of in a timely and secure manner so as to protect the privacy of individuals. Documenting the destruction of records can support the evaluation of record keeping arrangements.

7.7. Access to records associated with trustworthiness should be logged. Penalties and sanctions should be established and enforced for unauthorized access to, or use of, records associated with trustworthiness assessments to ensure that the information is used only for its intended purpose. Consideration should also be given to certain type of records (e.g. medical or psychological), for which the State might already have specific regulations in relation to record keeping.

7.8. A competent authority or licence holder can be designated to oversee record keeping in a centralized location, temporary maintenance and destruction of trustworthiness related documentation in accordance with State laws and regulations.

RECORDS OF ACCESS AUTHORIZATIONS

7.9. The licence holder is responsible for maintaining a current list or database of approved access authorizations. This list should be subject to the appropriate information security measures to ensure the confidentiality, integrity and availability of information. The list or database can only be viewed by individuals with a need to know and access to the list or database should be logged. Only authorized individuals should have the ability to modify data. Measures to prevent the falsification of data by those who can view the list or database should also be implemented.

7.10. Licence holders grant access authorizations for a designated period. The list or database of access authorizations should thus be continually reviewed and updated to reflect expiry dates of access authorizations, as well as to remove individuals who no longer have access authorization owing to changes in job functions, terminations of employment, resignations or retirements, or changes in trustworthiness determinations. Individuals should be notified well in advance of the expiry of their access authorization to allow sufficient time for the submission of renewal information, where necessary. Organizational changes, position changes and separation processes should be accompanied by notifications to the designated competent authority for the trustworthiness programme so that access authorization data can be updated accordingly and in a timely manner. Oversight evaluations should verify that access authorization data are being recorded and are up to date.

RECORDS OF ACCESS SUSPENSIONS, DENIALS, REVOCATIONS OR RESTRICTIONS

7.11. The licence holder is responsible for keeping records of suspensions, denials, revocations and restrictions of access authorizations for the period designated by the competent authorithy or State law. Such administrative actions can have implications for future applications for access authorization, and therefore these records should be maintained for future assessments. While managers should be informed of such administrative actions in order to have the appropriate restrictions implemented, the justifications for these actions (i.e. the suspensions, denials, revocations or restrictions of access authorization) might include sensitive personal information. The continued protection of this information should remain of utmost importance, with the information shared only on a need to know basis. Evaluations of the list of access authorizations should determine whether the administrative actions are being implemented in a timely manner so that only those individuals appropriately authorized are able to maintain their access to nuclear material, other radioactive material or sensitive information.

8. GRANTING, SUSPENDING, REVOKING AND REINSTATING ACCESS AUTHORIZATIONS

GRANTING OF AN ACCESS AUTHORIZATION

8.1. Once the competent authority has notified the licence holder that an individual has received a positive trustworthiness determination, the licence holder can then grant access authorization to the individual. Individuals who are granted positive trustworthiness determinations and receive access authorization are notified of their responsibilities and obligations under the trustworthiness programme. This notification should occur in a timely manner and should be documented in accordance with established procedures. The notification should provide the following information:

(a) The individual to whom the access authorization applies;
(b) The competent authority that has made the positive trustworthiness determination which allows the licence holder to grant access authorization;
(c) The areas where the individual has authorized access;
(d) The period for which the access authorization is valid;
(e) Any mandated reporting required by the State (e.g. change of partner or co-residents; financial difficulties; change of nationality; any new item on a criminal record) for the duration of the access authorization;
(f) Restrictions to access that might apply (e.g. medical conditions that restrict performing specific duties alone);
(g) A policy to abide by the conditions of access authorization of the licence holder, and where relevant, the competent authority;
(h) Conditions under which the access authorization can be revoked.

8.2. The competent authority should communicate to the licence holder any changes to an individual's trustworthiness determination in order to update the individual's access authorization.

Transfers of access authorizations

8.3. On the basis of established procedures and agreements, the State and competent authority could allow the transfer of a positive trustworthiness determination between licence holders in order to grant access to nuclear material, other radioactive material or sensitive information to temporary or permanent employees.

SUSPENSION OF ACCESS AUTHORIZATION

8.4. States should have a documented procedure to suspend a positive trustworthiness determination, when needed. The suspension of a positive trustworthiness determination should result in a suspension of an access authorization. In the case of the suspension of a positive trustworthiness determination, the individual concerned should be notified, and informed whether an appeal process is available.

8.5. Access control systems should be updated to reflect the revised status of the access authorization. The individual's supervisor or manager should also be informed, along with human resources and the medical department (where appropriate), to provide the appropriate support until all avenues of appeal are exhausted, if applicable.

REVOKING OF ACCESS AUTHORIZATION

8.6. States should have a documented procedure to revoke a positive trustworthiness determination where sufficient doubt exists in terms of the ongoing validity of the initial positive trustworthiness

determination. The revocation of a positive trustworthiness determination should result in a revocation of access authorization. In the case that a positive trustworthiness determination is revoked, the individual concerned should be notified, and informed in writing whether an appeal process is available (see paras 9.2–9.4).

8.7. Access authorization is no longer needed when individuals leave their employment, or they move to a different position that does not require the same access authorization.

8.8. Access control systems should be updated to reflect the revocation of access authorization. In the case where an individual's access was revoked as a result of a positive trustworthiness determination being revoked, the individual's supervisor or manager should be informed, along with human resources and the medical department (where appropriate), to provide the appropriate support until all avenues of appeal are exhausted, if applicable.

REINSTATEMENT OF ACCESS AUTHORIZATION

8.9. Reinstatement of access authorization is possible for individuals who have been reassessed and received a positive trustworthiness determination. For example, an employee who had left employment but has returned. Reinstatement of access authorization is also possible in the case that an individual has been successful in appealing a decision to revoke a positive trustworthiness determination. Access control systems should be updated to reflect the reinstatement of access authorization.

9. PROTECTION OF INDIVIDUALS SUBJECT TO TRUSTWORTHINESS PROGRAMMES

INFORMED CONSENT

9.1. The assessment process should have an overarching statement outlining the purpose of the assessment and the means by which the assessment will be undertaken. This statement should make clear that a trustworthiness assessment is voluntary, but that failure by the individual to provide consent to undergo an assessment is likely to result in the withdrawal of an offer of employment. If the individual is already employed, refusal of consent to undergo an assessment could result in the termination of employment if access authorization is needed for the job function. Where the individual provides consent to undergo a trustworthiness assessment, the individual should be made aware that he or she can withdraw consent at any time, although this might result in the termination of employment. Verbal consent should not be accepted; consent should be provided through physical or digital signature.

APPEAL PROCESS

9.2. If State laws permit, States might wish to establish an appeal process to allow individuals the possibility of appealing a negative trustworthiness determination or the revocation or suspension of a positive trustworthiness assessment. The competent authority responsible for trustworthiness determinations should establish an appeal panel to schedule hearings, take records and report on the outcomes of hearings. The competent authority should ensure that the persons who are overseeing the appeal process should be independent from those who reached the negative trustworthiness determination.

9.3. The appeal process should afford the opportunity to the individual to attend a hearing in person, if they wish to do so. The appeal process should indicate whether individuals are permitted to be accompanied, for example by legal counsel, a union representative or management. At the conclusion of the hearing, the individual should receive a written decision outlining the grounds on which the decision was reached unless national security restrictions apply.

9.4. Establishing a transparent and independent appeal process is more likely to instil confidence in the process and minimize the potential for legal challenges. Moreover, an appeals process will enhance established standards for trustworthiness determinations by ensuring accountability.

10. CRITERIA FOR REPORTING

10.1. A key component to ensure the continuing trustworthiness of individuals is to foster a culture that supports the monitoring and reporting of individuals' behaviour and actions, and encourages self-reporting. Management in particular should be encouraged to observe the behaviour of personnel and report any behaviour of concern or non-compliance with mandated reporting to the independent department addressing trustworthiness concerns. The licence holder should treat reporting as a legitimate and important function of the trustworthiness programme.

10.2. An effective trustworthiness programme should establish reporting procedures for individuals and for relevant departments (e.g. human resources, medical departments, nuclear security departments). These procedures should include the following chain of command for reporting:

(1) Individuals can report to management, to human resources or to the security department, directly or in an anonymous manner (e.g. through a reporting hotline);
(2) The human resources, security and medical departments or hotline should then report to an independent department that manages trustworthiness concerns;
(3) The independent department that manages trustworthiness concerns conducts an inquiry;
(4) The results of the inquiry are reported to the competent authority.

10.3. The competent authority will then determine if a reassessment of the trustworthiness determination is necessary. The reporting procedures should provide clear criteria for individuals to exercise good judgment in determining what and when to report. Reporting criteria can include indicators of aberrant behaviour that could potentially undermine nuclear safety and security.

10.4. The licence holder should develop a training programme to effectively educate all individuals on their responsibilities in the context of the trustworthiness programme, as well as the overall criteria of the programme. Training should consider cultural barriers to reporting, with such barriers being addressed directly and attempts made to diminish them in order to ensure active engagement in the trustworthiness programme. The training programme should not be delivered on a one time basis. Elements of the training programme should be included in induction arrangements (e.g. on-boarding), and individuals should be subject to refresher training after a given period.

DIRECT OBSERVATION

10.5. An effective trustworthiness programme fosters a nuclear security culture that encourages individuals to be observant of behaviour or activities that could be an indication of insider adversary actions. Such actions could include the unauthorized removal or movement of nuclear material, tampering with the containment of nuclear material or falsification of records. For direct observation to be effective, individuals should be capable of recognizing unauthorized activities and should be in a position to properly report the activities to the appropriate personnel using the designated chain of command. Once reported, confirmation should be provided to the individuals, indicating that their report has been received and is being investigated. The outcome of the inquiry should be confidential.

SELF-REPORTING

10.6. An effective trustworthiness programme includes policies and procedures for individuals to self-report on factors that could merit further evaluation, as defined in the trustworthiness programme on the basis of the State's laws and regulations. Self-reporting could include reporting information on arrests or criminal charges, convictions, changes in name or personal status (e.g. marriage, divorce, birth or adoption of a child), foreign travel, ongoing foreign contacts, financial problems, bankruptcy, change in citizenship, medical issues, treatment for mental illness, drug abuse or alcohol abuse.

10.7. The State or competent authority should establish the time frame for reporting, as well as the consequences for not reporting. The time frame for reporting personal changes could vary according to the change in question. For example, criminal or legal incidents might need to be reported in a more timely manner (i.e. depending on the nature of the offence) than a change in the individual's marital status.

REPORTING BY THIRD PARTIES

10.8. Part of an effective nuclear security culture is encouraging third parties (e.g. contractors, vendors, visitors) to be observant of any unusual behaviour or activities. Since third parties have their own chains of command, licence holders should make arrangements for the management of vendors or contractors to be capable of freely reporting to the licence holder.

CONFIDENTIALITY AND NON-RETALIATION POLICIES

10.9. Confidentiality and non-retaliation policies are important aspects of trustworthiness programmes. Reporting procedures should include confidentiality and non-retaliation policies to ensure that individuals will be treated fairly and that any information reported will remain confidential. These policies should also ensure protection against retaliation in the case of self-reporting, reporting behaviour of concern in good faith or participating in an inquiry.

10.10. The policy on non-retaliation should also stipulate actions that should be taken if concerns reported in relation to an individual's behaviour are deliberately false. The intended function of the legitimate activities that comprise the trustworthiness programme can be subverted by unscrupulous individuals for inappropriate reasons. Such individuals can falsely accuse personnel, or hide the malicious acts of other personnel. If not appropriately adressed, the unintended consequences of not addressing false reports, or failures to report inappropriate behaviour, can have a negative impact on the overall nuclear security culture.

PROCESS FOR CONDUCTING INQUIRIES

10.11. An inquiry process is necessary to examine information reported and to determine an appropriate response. The objectives of an inquiry are to gather information and facts, provide an opportunity to the individual under investigation to give input, and identify motivational or behavioural indicators (e.g. stress, financial irregularities, conflict, other workplace difficulties) in order to decide the appropriate response (e.g. report to the competent authority for reassessment, take employment actions, terminate employment). Inquiries should be impartial and thorough, and be completed in a timely manner. If not conducted correctly or in a fair manner, inquiries can negatively impact morale and trust among personnel, reducing the effectiveness and overall benefit of the trustworthiness programme. The inquiry process could include the following steps:

(1) Determining the need for an inquiry;
(2) Planning the inquiry;
(3) Conducting the inquiry;
(4) Reporting the inquiry results;

(5) Taking the appropriate action.

Determining the need for an inquiry

10.12. The first step in the inquiry process is to decide if an inquiry is in fact needed, which can be determined on the grounds of the information reported. The licence holder will determine the need for an inquiry on the basis of a number of considerations, such as whether the information reported meets the defined criteria of a behaviour of concern. When the licence holder receives reported information, the competent authority should be notified within the established time frame for the type of information reported. In some cases (e.g. reports of unauthorized removal of nuclear material, sabotage, misuse of sensitive information) the competent authority may decide to take over the inquiry.

Planning the inquiry

10.13. Effective planning ensures that the inquiry is properly conducted. The licence holder should determine the objectives and scope of the inquiry, the individual who will conduct the inquiry, the inquiry process and the time frame. The objectives and scope will determine the activities of the inquiry. In the case that the inquiry reveals other issues in addition to those reported in the original concerns, the individual conducting the inquiry could decide to include these additional issues and expand the scope of the inquiry, to initiate a separate inquiry, or to disregard these other issues and focus on the initial scope of the inquiry. Individuals appointed to conduct inquiries should be impartial and possess the necessary skills to conduct such inquiries. These skills will be judged on the basis of the individual's level of training, education and experience.

Conducting the inquiry

10.14. The individual assigned to conduct the inquiry should gather the relevant evidence and consider the nature of the report or concerns, in compliance with State laws and policies regarding privacy and access to information. The process can include interviews and document reviews (e.g. personnel files, records, logs, digital information, emails, text messages, computer files). Interviews of individuals under investigation should include a discussion on issues in relation to cooperation, confidentiality procedures, and the importance of providing truthful and honest information. Interviews of individuals in support of the investigation should include information on non-retaliation policies, and on whether the individual under investigation can access the details of the interview. Individuals under investigation should be provided with support through an assistance programme from the moment they are notified that they are subject to an inquiry.

Reporting inquiry results

10.15. Reporting of the inquiry results should contain factual conclusions that directly address the objectives of the inquiry, supported by the information that has been gathered. The report should

document the process, the information collected, the final determination and the justification of the conclusions.

Taking appropriate actions

10.16. Management should take appropriate actions on the basis of the final determination of the inquiry. Such actions could include the following:

(a) Allowing the individual to maintain their positive trustworthiness determination while management monitors the individual's behaviour and work performance;
(b) Revoking or reducing the individual's access authorization while management addresses the causes of the behavioural issues and monitors the individual's work performance;
(c) Revoking the individual's access authorization and making a request to the competent authority to revoke the individual's positive trustworthiness determination;
(d) Taking no action, if concerns are determined to be unsubstantiated, inaccurate or misunderstood, or if there is a valid explanation for the reported behavioural concerns.

11. AUDITS AND INSPECTIONS OF A TRUSTWORTHINESS PROGRAMME

AUDITS FOR TRUSTWORTHINESS ASSESSMENTS AND DETERMINATIONS

11.1. Trustworthiness assessments and trustworthiness determinations should be subject to audit to ensure that the appropriate assessment and determination processes were followed. Audits should be done on a predetermined sample size with cases selected at random.

11.2. The audit should consider whether the trustworthiness assessment and determination were conducted by suitably qualified and experienced personnel. Personnel that conduct trustworthiness assessments and determinations can be subject to bribes, which could result in the individuals who are undergoing assessments receiving false positive trustworthiness determinations. Access authorizations might therefore be granted in cases where they might not otherwise have been granted, increasing the potential for malicious acts by insider adversaries. Such issues could be mitigated through periodic or random audits of trustworthiness assessment and determinations, as well as through periodic trustworthiness reassessments of the individuals conducting assessments and determinations.

11.3. Audits can take the form of reviews conducted by a separate internal audit section of the competent authority or reviews conducted by an independent or national audit authority, including organizations with regulatory oversight. Where the review is performed by an internal audit section of the competent authority, audits should be conducted by personnel who are independent from those who conducted the original trustworthiness assessment or made the trustworthiness determination. Audits

should not be conducted by the supervisors of the individuals who conducted the orignal trustworthiness assessment or made the trustworthiness determination.

11.4. When a trustworthiness determination is under an audit, the licence holder should be notified. Where the trustworthiness determination was made on the basis of an inaccurate assessment, a new assessment should be conducted. For cases in which the positive trustworthiness determination is revoked upon reassessment, individuals should be informed in writing of the reasons for the decision (see paras 8.6–8.8).

REGULATORY INSPECTIONS OF THE TRUSTWORTHINESS PROGRAMME

11.5. To assess the trustworthiness programme established by the licence holder, the competent authority for the licence holder should conduct inspections at the premises of the licence holder to discuss procedures with the personnel responsible for implementing the trustworthiness programme and to discuss the perceptions of individuals (selected at random) in relation to the trustworthiness programme. The results of such inspections should confirm that the licence holder is implementing the trustworthiness programme appropriately.

11.6. Some inspections can be conducted remotely. For example, reviews of licence holder policies (e.g. social media, drug and alcohol testing, harassment and bullying) can be conclusive enough to avoid having to physically visit the premises of the licence holder.

11.7. All inspections should conclude with the production of a written report, which not only provides an overall view of the trustworthiness programme, but also indicates areas which need improvement, along with good practices.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[3] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLIE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME AND WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[4] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod. 1 (Corrected), IAEA, Vienna (2021).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev.1), IAEA, Vienna (2020).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 21, IAEA, Vienna (2013).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 36-G, IAEA, Vienna (2019).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Self-assessment of Nuclear Security Culture in Facilities and Activities, IAEA Nuclear Security Series No. 28-T, IAEA, Vienna (2017).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and Other Radioactive Material, IAEA Nuclear Security Series No. 38-T, IAEA, Vienna (2021).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), IAEA, Vienna (2016).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Recruitment, Qualification and Training of Personnel for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-75, IAEA, Vienna (2022).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, The Operating Organization and the Recruitment, Training and Qualification of Personnel for Research Reactors, IAEA Safety Standards Series No. SSG-84, IAEA, Vienna (2023).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessing Behavioural Competencies of Employees in Nuclear Facilities, IAEA-TECDOC-1917, IAEA, Vienna (2020).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018)

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities, IAEA Nuclear Security Series No. 11-G (Rev. 1), IAEA, Vienna (2019).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Managing Counterfeit and Fraudulent Items in the Nuclear Industry, IAEA Nuclear Energy Series No. NP-T-3.26, IAEA, Vienna (2019).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities, IAEA Nuclear Energy Series No. NP-T-3.21, IAEA, Vienna (2016).