WINS INTERNATIONAL BEST PRACTICE GUIDE

GROUP 1: Nuclear Security Programme Organisation

1.4

Nuclear Security Culture

Revision 3.0

WORLD INSTITUTE FOR
NUCLEAR SECURITY

Nuclear Security Culture

A WINS International Best Practice Guide

WHY YOU SHOULD READ THIS GUIDE

Experience in a wide range of organisations entrusted with the security of sensitive materials strongly indicates that a pervasive *culture* of security—as much as a robust security infrastructure—is essential to successfully lowering the risks associated with insider and external threats. This WINS International Best Practice Guide explains what nuclear security culture is, how it is created, and why it matters. It also sets out specific steps executive management can take to improve it.

A broad programme such as the one described here could substantially strengthen day-to-day security practices at nuclear facilities and lower the risks of nuclear material theft, sabotage, and loss of classified information. This guide offers guidelines on what such a programme should include. Every nuclear facility will need to develop its own programme, in consultation with the State regulator and other relevant stakeholders, according to its specific needs and circumstances.

This guide also includes the WINS *Employee Attitude Survey* which, when conducted, will give you a useful impression of your organisation's prevailing security culture and help you determine where to apply your efforts to achieve the greatest improvements. Our intention is to help you think through such issues and to ultimately contribute to a stronger security culture at nuclear facilities around the world.

About the Appendices

The WINS *Employee Attitude Survey* can be found in Appendix A together with the rationale for selecting particular questions to include in your survey.

Appendix B provides a five-level scale that will help you gauge the maturity of your organisation's approach to nuclear security culture.

About the Preparation of the Guide

This new revision of the Guide draws in part on ideas discussed at an August 2015 international workshop on security culture organised by Harvard University's *Project on Managing the Atom*. We thank Professor Matthew Bunn for his suggestions and for reviewing the document. The Guide also takes note of the real life experiences of security practitioners, managers of nuclear facilities, government agencies and regulators, including the results of other international workshops and meetings on security culture. Wherever possible, the Guide uses the same terminology as that found in the International Atomic Energy Agency (IAEA) Nuclear Security Series and Safety Series publications.

We Welcome Your Comments

We plan to update the information in this Guide frequently to reflect best practices and new ideas. Therefore, we ask that you read it carefully and then let us know how to improve it. If you need help or assistance with any aspect of this Guide, please email us. You can also contact us via the WINS membership portal.

Dr Roger Howsley
Executive Director
January 2016

Revision 3.0

ISBN: 978-3-903031-80-7

WINS Contact Information

World Institute for Nuclear Security

Graben 19

AT-1010 Vienna

Austria

Email: info@wins.org
Fax: +43 (0) 1230 606089
Phone: +43 (0) 1230 606083

www.wins.org

TABLE OF CONTENTS

WHAT IS MEANT BY NUCLEAR SECURITY CULTURE?

Fundamentally, ***nuclear security culture*** refers to the beliefs, understandings and practices that people in the workplace—from the board and senior executives to the general workforce—bring to security. Experience demonstrates that the culture of security is essential to successfully protecting nuclear and other radioactive materials from external and insider threat. In Security Series No 7, the IAEA says:

> *An effective nuclear security culture depends on proper planning, training, awareness, operations and maintenance as well as on the thoughts and actions of people who plan, operate and maintain nuclear security systems. An organisation may be technically competent while remaining vulnerable if it discounts the role of the human factor. Thus the human factor (including the upper tier of managers and leaders) is important to effective nuclear security.*

Culture can support—or hinder—any organisation's ability to achieve its goals, whatever they might be. Why is culture so important? Because it goes to the heart of the appropriate behaviours, right decisions and responsible practices that are essential in the workplace. In fact, having a culture that is appropriate to the kind of enterprise in which an organisation is engaged is one of the most important determinants of how effective or successful the organisation will be.

In an organisation with a strong security culture, staff believe that security threats are real, understand it is their responsibility to contribute to the security of the entire organisation, and adhere to security practices as a normal part of their daily work lives. If they observe an anomaly or hear something suspicious, they report it unhesitatingly to their supervisors. If they make a mistake themselves, they willingly own up to it, seek to understand how it occurred, and work actively to improve their performance. If they have ideas or suggestions for how to improve security, they share them with their managers and colleagues because they know such contributions are encouraged, respected and rewarded.

> Good security is 20% equipment and 80% culture.
>
> *Gen. Eugene Habiger, former commander of U.S. strategic nuclear forces*

In contrast, if the security culture is weak, the workforce may resent security features and do their best to ignore or circumvent them. They may also be reluctant to express concerns about aberrant behaviours and issues, materially increasing the risk for all concerned.

Many of the tools and techniques that have emerged from the effort to improve nuclear *safety* culture are directly relevant to nuclear *security* culture. Both disciplines play important roles in maintaining safe, secure operations and are closely linked in their underlying principles. Furthermore, both safety and security cultures are dependent on proper planning, training, awareness, operation and maintenance. Even a well-designed system can be degraded if the culture of the organisation allows poor procedures to persist or if it leads staff to believe they do not need to follow the procedures.

The Elements of Organisational Culture

Safety and security culture are based on the concept of overall organisational culture.

All organisations—whether they are families, social clubs, religious organisations, for-profit businesses, nongovernmental organisations, or governments—have an underlying culture based on certain values and beliefs. These, in turn, lead to certain kinds of attitudes and behaviours.

Beliefs, Values, Attitudes and Behaviours

An organisation's security culture is built on the beliefs, values, behaviour and attitudes of its senior managers and workforce.

1. Beliefs consist of ideas that each of us accepts as true. We have beliefs about all areas of our lives, from religion and morality to economics and society. We are not born with beliefs; rather, they are our deep-seated, personal responses to life's lessons and experiences. Organisations, too, develop beliefs as a result of experience and reflection. For example, as a result of their experiences in the nuclear sector, both WINS and the IAEA have come to believe in the fundamental importance of two propositions:

- Credible threats to nuclear materials exist at all times.
- Nuclear security plays a vital role in combatting these threats.

These two beliefs form the foundation of nuclear security culture. If they are not held strongly, an effective nuclear security culture will not exist.

2. Values are global, abstract principles that serve as guiding principles for our lives (e.g. freedom, honesty, equality, beauty, perseverance, harmony, etc.). A strong security culture would hold values such as:

- Being a learning organisation is important.
- Being accountable is important.
- Delivering high quality training is important.
- Security is the responsibility of every person in the organisation.

Organisations with strong nuclear security values repeat these messages regularly and expect all staff and contractors to uphold them.

3. Attitudes arise from an inner framework of values, beliefs and emotions and are developed over time. They consist of a person's likes or dislikes for anything and involve making judgments that can be positive, negative or ambivalent. They involve an emotional, verbal, behavioural or mental response to a task or person based on the individual's internal belief system.

4.Behaviours are the ultimate, tangible demonstration of an organisation's values, beliefs, and attitudes. To improve staff behaviour, senior management must clearly understand their own roles and responsibilities for security, know when and how to use their authority, and provide management oversight. They must also determine how they will motivate and improve staff performance and the degree to which staff will be involved in the decision-making process.

The following table demonstrates how security culture values and beliefs lead to certain kinds of behaviours.

Values & Beliefs	Resulting Behaviour(s)
A strong culture of security is crucial to protecting nuclear and radioactive materials.	The organisation's security policy, quality management system and change management processes help to ensure that all employees consistently demonstrate a strong nuclear security culture. The organisation takes a well-defined, well-documented approach to the management of security because it believes strongly that security culture is important.
Independent oversight strengthens security.	An effective, integrated oversight process—independent of line management and implemented as a recognised part of the management system—is in place.
To have a strong security culture, our organisation must value learning.	The board, management and workforce engage in continual learning to understand security issues better and to develop competencies at a level that is appropriate to each function.

Another, practical way of thinking about security culture is to consider the characteristics that contribute to it and to sub-divide the characteristics into five subcategories: leadership and motivation, accountability, professionalism and competency, integration, and learning and improvement. Following are some examples, based on IAEA guidance, for nuclear security characteristics.

Leadership and Motivation: Leaders have an enormous influence on staff performance; this is why nuclear security can only be truly effective when leadership clearly demonstrate their commitment to it through their words and actions. For instance, senior managers committed to building a strong security culture often use site visits as an opportunity to review and discuss security issues with local managers and staff. They also respond quickly to security needs such as purchasing equipment, improving management systems, providing training, or dealing effectively with an actual event. Leadership is important at all levels of the organisation, as a mid-level manager in some cases can create a sub-culture within his or her group that differs markedly from the culture senior managers are seeking to build.

Accountability: Nuclear security is most effective when all staff understand they are not only accountable for their own jobs, but that they also have a responsibility to contribute to the safety and security of the entire organisation. This requires that security roles and expectations be clearly identified for staff at every level and that security performance be reviewed during annual work appraisals.

Professionalism and Competency: Nuclear security demands that staff have the qualifications, skills, knowledge and training necessary to contribute to organisational security at a high level of professional competence. WINS promotes the need for professional certification for key roles.

Integration: Security processes must be integrated with all aspects of an organisation's management framework, including safety, emergency planning, operations, human resources and strategic planning.

Learning and Improvement: A strong nuclear security culture grows out of a commitment to continual learning and improvement. Applying best practices and lessons learned from within the organisation, as well as from other organisations, is an inherent part of this process. Regular self-assessments help the entire organisation understand why any security lapses have occurred and what to do to prevent similar lapses in the future.

Factors that Encourage a Strong Security Culture

Organisations can take a variety of actions in many different areas to improve their security culture. As the following figure demonstrates, all of these actions begin with - and depend upon - leadership.

Ensure Effective Leadership

In Nuclear Security Series No. 7 (Nuclear Security Culture), the IAEA explains that:

> *When leaders demonstrate they value nuclear security, the rest of the staff will, too. This helps to create a positive nuclear culture throughout the organisation. Another benefit is that leadership will increase their ability to obtain feedback on key topics and emerging issues.*

Nuclear security leadership is required from the State and regulatory authority, as well as from the organisation.

Government Leadership

Effective leadership begins with the government and regulatory authority. Site leadership will not have an incentive to improve their security culture if they do not understand the threats they face. Therefore, the government should brief site leaders on the gravity of the threats to nuclear materials and classified information, the need for operators to achieve an effective nuclear security culture, and the role they play in contributing to its success.

Require a security culture programme

The regulatory authority should require site directors to create and sign off on a programme for assessing and strengthening security culture. The programme should be developed in partnership with site leaders, not simply imposed on them, and they should be required to report regularly on their programme's progress.

Create a root causes process and lessons learned database

An enterprise-wide root causes and lessons-learned process (perhaps similar to that used by INPO for nuclear safety) should be established so that sites can learn from issues and incidents that arise at other sites. A database of security incidents at nuclear facilities—as well as at non-nuclear facilities if the incidents illustrate potential adversary tactics and capabilities or potential security vulnerabilities relevant to nuclear organisations—should be built and regularly updated. Information should include lessons learned that can be shared among all nuclear organisations. A programme to collect and analyse varying practices at different sites within the State should also be created so site management can learn from what works best and improve their performance.

Organisational Leadership

Organisations that achieve a strong, effective security culture share similarities in various important areas of management, including the Strategic Context, Organisational Management Systems, Comprehensiveness of the Security Programme, Performance Management, Employee Engagement and Attitudes, and External Stakeholder Engagement. Each of these areas can be further divided into elements that characterise operational excellence. Following are some examples of these elements, along with a description of what best practice looks like in each one.

1. Understand the Strategic Context

It is important to understand the strategic role that security plays in corporate governance. Following are some descriptions characteristic of organisations that understand and apply best practice.

Senior management see security as a corporate responsibility.

Senior management understand the importance of nuclear security in supporting business objectives and communicate it throughout the entire organisation. Because they see security as a strategic corporate risk that is part of the overall risk management framework, they have identified both internal and external threats to the organisation and designed and implemented security strategy and policies to mitigate them. Furthermore, senior management have identified their personal responsibilities, accountabilities and liabilities for nuclear security, and they require that individuals who hold senior positions with nuclear security accountabilities have demonstrable competences in this area.

Senior management have identified their business objectives and the regulatory requirements and incorporated them into the security strategy and policies.

Senior management are aware of the global nuclear security architecture, the special role played by the IAEA, and the important contributions of other international organisations and initiatives, such as the Nuclear Security Summit processes. They understand national regulatory requirements, communicate effectively with the regulatory agency, and periodically meet with the regulator. Furthermore, they have established clear security objectives and frequently discuss, review and update their organisation's security policy. They also appreciate how important it is to have a well-defined policy for rewarding and recognising staff who proactively contribute to security, and senior management have made sure that the entire workforce understands the importance that employee contributions make to the effectiveness of the security programme.

Senior management have defined their security expectations and are committed to achieving them.

Senior management have committed the necessary resources to fund security at an effective level. They adhere to the same security policies and procedures required of lower-level staff, and they regularly review organisation-wide performance roles and responsibilities to ensure that key security responsibilities are being met. They assess security performance in the field by conducting walk-throughs, listening to staff, and observing the work that is being conducted. They provide constructive feedback to reinforce expected behavior and take action to correct deficiencies. They also benchmark the organisation's performance by looking at how other organisations perform similar tasks.

Senior management make security a high-profile issue and communicate this commitment effectively.

Senior management regularly communicate with each other and with staff about security issues on such topics as emerging threats, professional conduct, personal accountability, vigilance, adherence to procedures, opportunities for improvement, and teamwork and cooperation. They consistently brief staff about nuclear security concerns and emerging issues and facilitate group discussions about the reality of the threat and its potential consequences. They ensure that staff know how to translate top-level expectations into operational performance and continually emphasise the importance of developing a questioning attitude, acting conservatively, reporting concerns, and seeking advice when nuclear security issues arise.

Furthermore, senior management demonstrate the value they place on two-way communication and quickly address any potential communication blockages. Whenever possible, they inform staff about the context for the decisions and high level policy and organisational changes they make. They also place a high value on the quality of written communications and ensure that all procedures and guides are well-written, easy to understand, and user-friendly.

2. Implement Supportive Organisational Management Systems

It is important to put organisational management systems in place that support nuclear security. Following are some descriptions characteristic of organisations that do so.

Senior management integrate security into the organisation's overall management system.

Senior management recognise that security is a strategic risk, so they integrate it into the wider management system in the same way that they integrate safety. They have established clear lines of authority, resources and accountability for security, safety and emergency planning, as well as procedures that guide interactions among them. Senior management have created an Executive Sub-Committee on Security (as well as for Safety), regularly emphasise that their goals for safety, security and operations are equally important, and demonstrate these values in their staff policies and communications.

The organisation's governing body has put a written Security Policy in place.

The organisation's board of directors (or other relevant governing body) view security as a central component of business success. Consequently, they have created a written security policy that demonstrates organisational commitment to nuclear security to all stakeholders and defines security accountability throughout the organisation. The policy clarifies board and management responsibilities for security delivery and oversight, establishes key organisational priorities for security, and provides guidance to management on risk tolerance, processes, and performance standards. The policy also specifies the regulatory and/or voluntary undertakings that management must meet and the board's reporting and information requirements. Furthermore, the policy clarifies who the delegated authorities are, the matters upon which management must consult with the board, and the timeframes in which such consultations must take place.

Senior management have created a well-defined security management system (SMS) programme.

Building on the security policy, senior management have clearly identified their strategic objectives and risk appetite for security and have created a written security management system programme that identifies the organisation's approach toward such issues as:

- External Stakeholder Engagement and Communications
- Performance Testing and Effectiveness
- Regulatory Engagement and Legal Issues
- Corporate Oversight and Reporting
- Financial/Budget Provision and Requirements
- Information Security and IT Systems and Cybersecurity
- Human Reliability and Personnel Security (vetting and aftercare)
- Employee Awareness, Engagement and Professional Development/Certification
- Physical Protection and Facility Infrastructure, including Access Controls
- Emergency Planning and Response, including Personnel Evacuation

Senior management have clearly identified organisational roles and responsibilities for security.

Senior management have clearly determined and documented who is responsible for various aspects of the security programme using a tool like the RACI (**R**esponsible, **A**ccountable, **C**onsult and **I**nform) technique. As a result, all personnel in the organisation know who is Accountable, or ultimately responsible, for the security programme and has yes/no decision making authority. They also know who is Responsible for carrying out and implementing particular aspects of the programme, who needs to be Consulted before a decision is made, and who needs to be Informed after the decisions and/or actions have been taken.

Senior management emphasise that quality assurance and record keeping are a priority.

Senior management ensure that the organisation's security processes are prepared, documented and maintained in accordance with recognised quality assurance standards. They strongly enforce the quality assurance measures they have set and periodically evaluate the procedures against good practices for the industry. They also understand the need to publish Assurance Reports and are committed to doing so.

3. Implement a Comprehensive Security Programme

Organisations must ensure that they carefully think through their security programme and ensure it adequately addresses all of the major issues. Following is a description of best practice that typifies effective security programmes.

Senior management make sure that physical protection measures are well understood and correctly implemented.

Senior management understand that effective physical protection systems combine human, procedural and technical resources to ensure deterrence, detection, delay and response functions that are capable of mitigating both the internal and external threats identified in the regulator's design basis threat. Consequently, they make sure their organisation's physical protection systems follow the concepts of a graded approach and defense in depth and that they are flexible enough to adequately respond to periods of increased threats. Senior management also ensure that physical protection provisions are coordinated with measures implemented for other risk management purposes and that the arrangements are tested periodically to ensure their effectiveness and sustainability.

Senior management ensure that cybersecurity management procedures have been clearly identified and implemented, and they carefully oversee them.

Senior management ensure that appropriate measures for the security of IT&IC systems have been implemented, are overseen by an appropriate authority, and are being operated in accordance with written procedures. They make sure that the processes and protocols for operating computer systems are based on internal experience and feedback combined with industry best practices and that the organisation's cybersecurity policies and expectations have been clearly communicated to all employees.

Senior management ensure that information security policies and procedures are implemented effectively.

Senior management understand the national requirements and business expectations for controlling sensitive information and make sure they are implemented into security policies and protocols for classifying and handling sensitive information. They periodically review the policies and controls that guide information security management and instigate audits to verify that access to sensitive information is restricted to those who need it to perform their duties, have the necessary authority, and have been subjected to a trustworthiness check commensurate with the sensitivity of the information.

Senior management have put a comprehensive insider mitigation programme in place that is implemented effectively.

Senior management have developed a comprehensive insider mitigation programme that is effectively coordinated and implemented among all departments and activities. The programme comprises a comprehensive human reliability programme for security that includes personnel screening processes subject to oversight and auditing. Personnel also receive training in how to identify aberrant behaviours that may suggest an insider issue, and the importance of reporting them. Insider mitigation programmes should also include constant surveillance of sensitive items or areas that need to be protected, and arrangements to limit human access to them to the minimum necessary for operations.

Senior management ensure that security interfaces closely with safety and operations.

Senior management ensure that the interface among safety, security and operations is managed in a risk-informed, balanced way and that the synergies and conflicts among them are considered together to avoid negative impacts during operation. Designers and operators of safety and security systems (including IT&IC systems) work together to ensure that security measures do not compromise safety features and vice versa. Workflow is well-planned so that the integrity of the nuclear security system is maintained at all times. Staff are actively involved in the identification, planning and improvement of security-related work and work practices, and resources are matched to the demands.

4. Engage Employees in Security

Draconian security measures that make staff feel their sites are being turned into prisons or that security measures make it impossible for them to operate effectively are counterproductive. Instead, the goal must be to enable staff to see safety, security and doing their job as an integrated whole because each element is essential to the overall success of the organisation.

Educate staff about the threat

Belief that the organisation faces credible threats is fundamental to a strong nuclear security culture. If staff do not believe the threats are real, they will not take security seriously. Because complacency is the enemy of vigilance, it is important that staff understand no security system is invulnerable and that adversaries may well find and exploit a vulnerability at their facility.

This is why leadership need to provide regular threat briefings to all staff with responsibilities for nuclear or other radioactive materials. In the majority of cases, the threats will relate to the possibility of sabotage or theft of nuclear material and other radioactive materials. In the case of facilities that process or store HEU or separated plutonium, the briefings should describe the real efforts terrorists have made to seek nuclear weapons, the plausibility that terrorists will make a crude nuclear bomb, the thefts of nuclear material that have actually occurred, and real cases where insiders and outsiders have defeated security measures at guarded facilities (both nuclear and non-nuclear).

For those who handle classified information, the briefings should also describe the myriad threats to classified information—from traditional spying to cyber-hacking. The briefings should be as realistic and engaging as possible, but not too long. Briefings that staff perceive as insulting to their intelligence will undermine their commitment to security.

Include staff in decision making

To ensure buy-in as well as understanding, staff should be invited to assist in developing and improving the security system. Ways to incorporate staff into this process include holding periodic security workshops and exercises, developing a Continual Process Improvement programme, and encouraging group self-assessments. This inclusive approach benefits staff in numerous ways. For example, it gives them a sense of ownership in the process, reinforces their appreciation for security system procedures, and increases their willingness to adhere to them.

Determine security competencies and accountabilities

Senior management must set clear accountabilities and competencies for nuclear security professionals, managers and staff and review them regularly. Each staff member needs to understand his or her personal responsibilities, know how they interconnect with the responsibilities of others, and have the necessary competencies to meet the high professional standards and behaviours required by a strong nuclear security culture. When responsibilities have been established, an assessment of each staff member's security performance can be included in annual performance reviews. These need to include leading performance metrics, such as participation in security exercises, the completion of training, and other activities that build professional competence.

Create incentives

The impetus to cut corners on security is strong at multiple levels of the enterprise. By and large, employees do what they have incentives to do. Every hour an employee spends following security procedures is an hour not spent on other activities that may be more likely to lead to a raise or promotion. This is why it is important to provide additional incentives, such as bonus payments, when employees take proactive actions to observe and resolve security issues. Management could also offer a security hero award regularly (e.g., once a month or once a quarter) to an employee who has made a particularly significant or creative contribution to security. Because effective security requires team effort, awards should be offered for the best team performance in security as well.

Make security simpler and more convenient

The more inconvenient, intrusive, complicated, and time-consuming security rules and procedures are, the less consistently they will be implemented and the less effective they will be. If staff see a rule as needlessly burdensome and pointless, they are likely to ignore it. This creates a culture in which people pick and choose which security rules they will follow and which they will not. To avoid such circumstances, staff need to understand the underlying threats and vulnerabilities that led to the establishment of particular rules in the first place. And management need to cut back rules that are no longer appropriate to the security and operational environment.

Because people often forget to do what they are supposed to do, it is always best practice to make the secure option the one that happens automatically to as great an extent as possible. For example, rather than relying on staff to remember to lock a door, the door should be designed to lock by itself. Making security simpler and more convenient makes it more effective.

Leadership should also create a process whereby staff can nominate particular rules as needlessly burdensome and make suggestions for alternative approaches. Leadership should take action on these suggestions and publicise the results. If the suggestion was not made anonymously, they could also publicly reward the employee who made it.

Create red teams to find and fix vulnerabilities

An important part of the process of increasing security is identifying and fixing site vulnerabilities, and staff can play an important role in this regard. Leadership should set up *red teams* whose responsibility is to think like a hacker or adversary who is trying to defeat the security system. What avenues could adversaries use to carry out an attack? What kind of security measures would be most important in stopping their success?

Mechanisms should also be created for compiling, analysing, and sharing the results of the teams' work so that a vulnerability found in one place can be addressed and repaired in other places as well. An award could be given to the team that finds and contributes to fixing the largest number of credible vulnerabilities.

Commit to effective communications

The commitment to creating a positive security culture cannot be a one-time-only process. This is why senior management should develop an effective, continuing communications programme that makes security a high-profile issue. Its tasks should include regularly briefing staff on nuclear security concerns and emerging issues and reinforcing organisational values and expectations by publicising and rewarding individual achievements in enhancing security.

To reinforce the importance of security awareness among the workforce, the communication programme should promote security awareness, build understanding, and facilitate communication on security topics among colleagues and between staff and management. One way to do this is to facilitate group discussions and encourage informal co-worker discussions about the reality of the threat and the potential consequences should an incident occur.

The communication programme needs to educate staff about how to make individual and collective contributions to nuclear security culture and how to translate top-level expectations into operational culture so nuclear security becomes a respected, organisation-wide value that is integrated into routine work practice. The programme also needs to emphasise the importance of developing a questioning attitude, acting conservatively, reporting any concerns, and seeking advice when nuclear security issues arise.

> Open communication is absolutely critical. If we have an organisation that does not want to hear about problems, then that is exactly what you will get—problems!
>
> —Thomas D'Agostino,
> Former Under Secretary for Nuclear Security and NNSA Administrator, US DOE

It is important that senior executives create communications channels such as question-and-answer sessions, a telephone hotline, and discussion forums where staff receive prompt notification of incidents and feedback on security issues. Topics for on-going discussion might include emerging threats, professional conduct, personal responsibility, vigilance, adherence to procedures, opportunities for improvement, and teamwork and cooperation.

Additional tools that could be used to communicate with staff might include:

- Open meetings led by senior management
- Briefings by section heads
- Lunch-and-learn discussions
- An intranet security node
- Email communications
- An awards programme
- Promotional items inscribed with security values

Implement engaging education and training programmes

Leadership should commit to being a learning organisation in which training in security culture is included in site induction, formal refresher courses, on-the-job training and emergency exercises. Leadership should also work to create a collaborative workforce in which informal learning arises from the day-to-day sharing of insights and experiences.

Although security training is very important, it is often ineffective. One of the reasons for this is that such training often consists of nothing more than lectures about rules and procedures. The problem with this approach is that listening to a lecture (or watching a video of a lecture) is one of the least effective ways to learn new information. Furthermore, people have difficulty remembering a list of rules and procedures if they are divorced from the reasons for them. A much better approach is to tell stories, either true stories or realistic-seeming ones, because they help people remember better and do a better job of motivating them to act. It is especially effective to use active learning approaches that encourage participants to come up with their own ideas and solutions.

This is why it is important to establish security training programmes that include real stories about terrorists who have actually tried to obtain nuclear weapons and the materials to make them, real cases of sabotage or the theft of nuclear and other radioactive material, and examples of adversary teams that have found vulnerabilities in security systems. Training should also include real cases of when and how important information has been compromised, of how important it is to correctly classify information, and how the security procedures employees are asked to follow help to prevent such problems from occurring.

Emphasise communication, learning and corrective actions over retribution

Fundamentally, any serious concern—whether it stems from safety, security, financial mis-management or other aspect of corporate policy violation—has the potential to create serious reputational damage if it remains latent, unresolved or hidden. This is why leadership should proactively work to build a culture in which incidents and problems are seen as opportunities to learn and improve, rather than as moments for finding and firing those who are to *blame.*

Belief that reporting incidents will lead to punishment (or be completely ignored) greatly diminishes the staff's willingness to share their concerns, resulting in a situation in which leadership is unaware of emerging issues and fails to obtain feedback on key issues. Administrator of the U.S. National Nuclear Security Administration Thomas D'Agostino (2012) said that:

> *Leadership needs to ensure that their entire organisation understands that we want to hear about problems. Not only do we want to hear about problems, but everyone needs to also understand that it is their obligation to bring problems to our attention. With this openness there also needs to be reassurance that leadership will not "shoot the messenger." You have an obligation to the security of your nation and to the security of every other nation in this room to incentivise honesty and openness.*

This is why communication, learning, and corrective actions should be emphasised over retribution in all but cases of willful misconduct or repeated negligence. It is also important that senior management consider the information they receive in a timely manner and act on it promptly. The reporting of concerns should be encouraged through normal line management channels.

Many organisations believe that employees who are struggling with alcohol or drug abuse, experiencing emotional or financial problems—or who have other stresses in their lives—should be offered help via employee support programmes rather than being punished or fired. This approach can be highly beneficial to both the individual concerned and the organisation because it can reduce potential resentment and retaliation and encourage employee trust and loyalty.

Create a Strong Whistleblowing Programme

The reporting of serious concerns, often referred to as *whistleblowing*, empowers employees to report legitimate and serious concerns pertaining to health, safety and security, as well as to environmental damage, a criminal offence, or the covering up of wrongdoing. To enable such a process, employees must have confidence that their report will remain confidential and that their legal status will be protected. Whistleblowing programmes must not only protect those who legitimately report wrongdoing, but also those who are wrongly or falsely accused, from undue negative repercussions.

A whistleblowing policy is a commitment to the highest standards of ethical, moral and legal business conduct, and it is especially important in nuclear organisations. This is because insiders with access rights, intimate knowledge of a facility, and authority over staff have the ability to bypass dedicated security measures and compromise cybersecurity, material control and accountancy, technical security features and more. They also have the time to plan an event in coordination with outside terrorist groups. It is an individual's peers who are best placed to notice a colleague's unusual behaviour, sudden changes in attitude, or performance anomalies; in other words, signs that may point to the possibility that the colleague could become a threat.

> A strong organisation—one committed to continuous improvement—needs to develop a workforce that promotes a degree of skepticism, a questioning attitude and a desire to get into the details.
>
> Thomas D'Agostino

Understand the challenges

Encouraging employees to report concerns is inherently challenging. Although employees are the first line of defence when it comes to keeping their fellow workers, communities and organisation safe and secure, there are often strong cultural, legal and employment issues that make employees reluctant to report on their colleagues. Brandon Gaille, an American business blogger, says that among those who see wrongdoing and choose not to report it, 46% make such a decision because they are afraid of being retaliated against.

> *Even though reward programs are in place and laws protect whistleblowers in several nations around the world, it is a lot easier to ignore a whistleblower, silence them or discredit them, than it is to praise them.*

And yet, as Gaille explains:

> *Whistleblowing by its very nature is being more loyal than those who are committing the active wrongdoing in the first place. It's someone who has worked for an agency or company for a long time, believes in the mission, and has a good job performance. That's the ethics we want in the workplace, yet as a society we question the ethics of whistleblowing.*

Understand board responsibilities to create a whistleblowing policy

It is the board's responsibility to establish a clear whistleblowing policy and to provide careful oversight of the programme. From a legal perspective, the board must ensure it protects employees from damages as a result of legitimate whistleblowing so that the organisation does not face liability or breach of legislation. From a moral and ethical perspective, the board must ensure that the organisation creates standards of behaviour that are clear to all stakeholders. From a practical perspective, the board must ensure it provides safe mechanisms for reporting serious concerns within the organisation itself.

The policy must state that employees have the obligation to express their legitimate concerns about any perceived ethical, moral or performance-related matter. The board should publish its policy and make sure that all employees receive a copy of it.

Because a whistleblowing programme often involves serious allegations of wrongdoing, the board should establish an independent audit committee and regular audit protocols to ensure that:

- The organisation acts in accordance with State legislation.
- All officers and employees act in an ethical and legal manner.
- All stakeholders are treated fairly, with dignity and respect.
- All allegations are investigated thoroughly, professionally and promptly.
- Those found guilty are disciplined quickly, firmly and fairly.
- Those for whom the suspicions prove to be unfounded are treated fairly and suffer no long-term repercussions
- Whistleblowers receive private and/or public recognition when it is safe to do so.
- Staff understand that the organisation expects them to report, that those who do are treated fairly, and that a fair process is in place to investigate and assess the information.
- The company is seen to promote an ethical approach to business.

To build staff trust in, and adherence to, the programme, all employees and contractors should be given induction training when they are first recruited and receive regular refresher courses thereafter. They should know the process for reporting security policy violations and how to use it. To make the process as easy as possible, the organisation should have a confidential telephone number available 24 hours a day. Furthermore, a senior, independent manager who regularly reports the results to the CEO should investigate the reports, and the board should be apprised of overall trends and any actions being taken by management.

In the final analysis, the success of a whistleblowing programme depends on the presence of a vibrant security culture in which everyone understands that the threats are real; that it is in their best interest to do whatever they can to protect themselves, their co-workers, their families and their communities from harm; and that leadership will welcome, respond to, and reward reported incidents.

5. Manage Performance

Leadership should ensure that realistic tests are conducted of security performance against intelligent adversaries who are attempting to find ways to challenge the system. These should not only include force-on-force exercises against outsiders, but also tests of the protections put in place to defend against insiders. When staff participate in such tests, they become particularly aware of the tactics potential adversaries could use and how challenging such tactics can be to defeat.

Conduct force-on-force exercises

Many security systems work well on paper or in computer simulations but poorly in the face of an intelligent adversary thinking of clever ways to overcome them. Regularly carrying out force-on-force tests of how the system works in response to an outsider intrusion helps to demonstrate performance, reveal vulnerabilities that need to be addressed, train guard forces and other security staff, and strengthen awareness of the threat and of the site's vulnerabilities. Such exercises should include site self-assessment, as well as assessment by national regulators.

Conduct tabletop exercises

Tabletop exercises should be conducted to help participants envision how outsider or insider adversaries (or both) might try to defeat the site's security systems and how to improve protection against those tactics. In a tabletop exercise, participants are given a hypothetical incident in which events happen in simulated/compressed time; they must then make informed decisions based on the information they receive at different times during the event.

Participants are assigned a role in the exercise that either matches their occupation or is intentionally different from it. For example, a police commander may be asked to take on the role of facility director and vice versa. It is important that the scenario be both credible to the participants and challenging; to have any validity, the responses must be based on existing procedures and resources. All exercises should be performed to help participants *learn* from their experience, not to apportion blame or criticise individual or group performance.

Use metrics and indicators

To determine how effective the security culture programme is, it needs to be measured. This typically starts with key performance indicators (KPIs) that help to identify potential problem areas, stimulate actions, document management efforts, and reinforce improvements in behaviour. KPIs should be based on a realistic assessment of cause and effect. They should adequately map and identify causal linkages (root causes, precursors, events and outcomes) and consistently, accurately and reliably measure what they are supposed to. They should also provide information that is relevant to required management decisions and actions, facilitate accurate and detailed comparisons, and lead to correct conclusions. One of the most important requirements is that the personnel who are responsible for implementing change can understand them.

KPIs are considered to be either lagging or leading. **Lagging** indicators describe events or incidents that took place in the past, such as the number and type of security incidents. They generally indicate little about what an organisation is doing to implement improvements. In contrast, **leading** indicators focus on future performance and continuous improvement.

They include such measures as:

- Training programmes
- Employee attitude surveys of security culture
- Peer reviews
- The results of exercises and drills

Determining which KPIs to use and what the balance should be between lagging and leading metrics is important. If the frequency of security incidents is small, lagging indicators are unlikely to provide much useful information about the effectiveness of the security culture programme. This is why it is important to use a balance of lagging and leading indicators to gain a meaningful understanding of the programme's performance.

Evidence from the management of health and safety (both nuclear safety and occupational health) is that more mature organisations (i.e., those that have moved beyond compliance monitoring) make better use of leading metrics to help identify potential problems before they become failures or incidents. The ratio is often about 70:30. These organisations also ensure that the metrics are fully integrated into their risk management arrangements and aligned to their organisational priorities and objectives.

A further lesson from health and safety performance management is that it is highly desirable to establish a multidisciplinary team to identify the most appropriate leading indicators to use. This is important because the root cause of incidents (both safety and security) often lies in organisational culture, structures and processes (e.g., people, systems, policies and procedures) as well as technical issues (e.g. equipment and resources).

Conduct self-assessments of security culture

Although beliefs, principles and values provide the underpinnings for a strong security culture, it is not always apparent what they are. This is because they often operate at an almost unconscious level. When an organisation faces a changing environment or has identified the need for improvements in the way things are done, an established culture may impede progress unless it, too, is changed. Before methods can be devised and implemented for effecting change; however, it is important to know what the baseline is. This requires undertaking a formal self-assessment process to proactively identify an organisation's security beliefs, principles and values.

In its new draft document on Security Culture Self-Assessment (2014), the IAEA says that:

> *Security culture self-assessment plays a key role in developing and maintaining an awareness of the strengths and weaknesses of the organisation's nuclear security culture. Due to their heavy focus on perceptions, views and behaviour at all levels of the organisation, regular assessments help managers to understand the reasons for an organisation's patterns of behaviour in certain circumstances, to devise optimal security arrangements, and to predict how the workforce may react to the unknown.*

Such a review should draw on performance indicators, reviews of events, personnel survey data, and the results of relevant internal audits. Assessments should evaluate how well actions are being completed and how effective they are. They should be designed to provide people who are responsible for controlling the risks with accurate, useful and timely information. Taking such actions will help to reduce the likelihood that complacency will lead to organisational drift away from security excellence.

Methods of self-assessment

Organisations can use a variety of methods to assess their security culture, including surveys, interviews, and onsite observations. The most common method is probably a survey. An organisation may already conduct surveys on topics like overall employee satisfaction, corporate culture, compensation and benefits, and health and safety. Larger nuclear organisations may have the in-house expertise to implement surveys; others may need to appoint specialist external consultants to provide this service.

In contrast to general employee satisfaction surveys, security culture surveys are currently far less common. One reason for this is that organisations seldom focus on the role that employees play in overall security arrangements; instead of encouraging them to think about the rules in depth or to comment on their applicability, organisations simply require employees to follow security rules. Another reason may be that security arrangements are usually perceived as classified, so leaders may believe that engaging with employees on security issues could compromise confidentiality and put the organisation at risk.

Clearly, such obstacles cannot be justified if the overall objective is to establish a proactive, organisation-wide security culture. Employee views about, and support for, security are important and need to be understood. (Appendix A of this Best Practice Guide provides further information on the design and conduct of an Employee Attitude Survey for Security.)

6. Engage Effectively with External Stakeholders

Another facet of security culture is the relationship that the organisation has with its external stakeholders. These relationships are the responsibility of senior management. Following are some characteristics of organisations that engage effectively with their external stakeholders:

Senior management work effectively with the regulatory authority

Senior management frequently meet with the regulator. The interagency processes are streamlined, and senior management consistently report any nuclear security incidents that might have occurred to the regulator; in turn the regulator and/or the intelligence agencies shares appropriate information about vulnerabilities and threats with the organisation in a timely manner. Following the results of self-assessments, senior management regularly update the regulator about the organisation's security culture.

Senior management engage effectively with civil society

Senior management understand the importance of building trust and communicating effectively with their civil society stakeholders, including the media. They take a need to share approach toward security information rather than a need to know approach, and they communicate regularly with their civil society stakeholders in writing via the website, brochures, newsletters, corporate social responsibility (CSR) reports and more.

Senior management also engage face-to-face with their civil society stakeholders using such methods as questionnaires, focus groups, citizens' panels, and formal stakeholder dialogue meetings. Senior management listen to concerns and feedback from members of the local community and other concerned stakeholders and adjust their plans, processes and approaches—to as great an extent as possible—as a result. In addition, senior management receive training in how to communicate effectively with the media—both under normal conditions and during an emergency event.

Senior management communicate, coordinate and exercise effectively with offsite emergency responders.

Senior management have identified the offsite organisations, agencies and decision makers who would be involved in an emergency response and put written agreements/memoranda of understanding in place with them to facilitate their assistance, communication and timely response to an incident. Command, control and coordination plans have been put in place between these multiple agencies and mutually agreed. Offsite and onsite forces regularly exercise and train together, and lessons learned are incorporated into the procedures.

Together, all of the actions and recommendations described above when implemented will lead to an organisation with a strong security culture, for the benefit of its own corporate objectives and the safety and security of employees and off-site communities.

Suggestions for Further Reading

Bunn, Matthew. (2005, July 1014). Incentives for Nuclear Security. Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management. Phoenix, AZ. http://belfercenter.ksg.harvard.edu/files/inmm-incentives2-05.pdf

Bunn, Matthew, and Sagan, Scott D. (2014). *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes*. Cambridge, MA: American Academy of Arts & Sciences. https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderthreats.pdf

Gaille, Brandon. (2015, January). 22 Important Whistleblowing Statistics. http://brandongaille.com/22-important-whistleblowing-statistics/

D'Agostino, Thomas. (2012, December 5). Remarks to the Nuclear Regulatory Commission International Regulators Conference on Nuclear Security. (Provides a useful discussion of the importance of both questioning and reporting.) http://www.nnsa.energy.gov/mediaroom/speeches/nrcconfremarks120512

IAEA. (2014). Security Series No. XX: *Self-Assessment of Nuclear Security Culture in Facilities and Activities that Use Nuclear and/or Radioactive Material*. (Draft Technical Guidance). http://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst026.pdf

IAEA. (2008). Nuclear Security Series No. 7: Nuclear Security Culture. http://www-pub.iaea.org/books/IAEABooks/7977/Nuclear-Security-Culture

INPO. (2013, April) Traits of a Healthy Nuclear Safety Culture http://nuclearsafety.info/wp-content/uploads/2010/07/Traits-of-a-Healthy-Nuclear-Safety-Culture-INPO-12-012-rev.1-Apr2013.pdf

Khripunov, Igor (2015, June) A culture of security: Focus for the next Nuclear Security Summit? http://thebulletin.org/culture-security-focus-next-nuclear-security-summit8428

Reason, James. (1997). Managing the Risks of Organizational Accidents. Aldershot, UK: Ashgate.

Tobey, William, and Zolotarev, Pavel. (2014, January 13). *The Nuclear Terrorism Threat*. Pattaya, Thailand. http://belfercenter.ksg.harvard.edu/files/nuclearterrorismthreatthailand2014.pdf

WINS Best Practice Guides

2.1 Threat Assessment
2.3 Information Security for Operators: Challenges and Opportunities
2.4 Communicating Security Information: Striking a Balance
3.1 Developing Competency Frameworks for Managers with Nuclear Security Accountabilities
3.2 Human Reliability as a Factor in Nuclear Security
3.4 Managing Internal Threats

World Law Group. (2012). *The Global Guide to Whistle-Blowing Programs.* http://www.theworldlawgroup.com/wlg/Handbooks_Guides.asp

APPENDIX A:

Security Attitude Survey

WINS has created this Employee Attitude Survey on Nuclear Security Culture as a tool to help senior management understand what constitutes best practice and what their organisation's current attitudes toward security are. The model draws on international best practices for conducting employee surveys; guidance on nuclear security and safety from the International Atomic Energy Agency (IAEA); and information published by INPO and other organisations, such as the Centre for the Protection of National Infrastructure (CPNI) in the UK.

The WINS survey can be used as an overall model, but organisations should adapt the questions to fit their specific needs. To avoid any accusations of self-interest, the Security Department should NOT conduct the survey. It may be advisable, therefore, to ask an independent organisation or consultant to manage the process.

Rationale for conducting employee surveys on nuclear security

Experience demonstrates that a positive culture of security is essential to protect nuclear materials and facilities. Such a culture consists of the beliefs, understandings and values that people in the workplace bring to security; these, in turn, form the basis of the actions (behaviours) that they take in their jobs. Because belief, understanding and values often work at an almost unconscious level, it is important to take proactive steps to elicit what they are. One of the most effective ways to accomplish this is to conduct an Employee Attitude Survey. The information obtained from this process gives organisations the ability to create—or revise—training, policies and programmes that meet their strategic goal of ensuring that nuclear security culture remains strong over time.

Conducting the Survey

The WINS Employee Attitude Survey is structured to provide information about the overall organisation as well as about individual departments. This enables organisations to compare the differences among attitudes in different departments, as well as to identify best practices and problem areas. Following is a discussion of the steps that need to be taken before, during and after the survey to ensure its success.

Step 1: Establish objectives

The first step in developing an Employee Survey is to establish the survey's objectives. The goal in this endeavour is to ensure 1) that the survey accurately reflects employees' attitudes towards security and 2) that the results are used to inform the organisation's overall business objectives. The results will enable you to review/revise your Nuclear Security Programme, the training that employees receive in nuclear security, and the way you communicate with your employees. To obtain these objectives, you need to collect quantitative data that enables you to compare results in different areas and that also identifies trends over time so you can see if improvements are being made.

Step 2: Gain stakeholder buy-in

You need to identify all key stakeholders in your organisation to ensure tangible support for the survey and help it run smoothly. Senior management and any trade unions or staff representatives should be included in it. Ask a senior member of the executive team (preferably the CEO) to circulate a letter/memo to colleagues that is in favour of the survey and asks them to support its completion within their areas of responsibility. Keep stakeholders involved throughout the process.

Step 3: Define the audience

You need to decide on the audience for the survey. For example, will it be distributed to all employees, including senior management, the general workforce, and contractors who work in the organisation? Or will it be distributed only to a subset of the workforce? The answer to this question will influence the methods you use to design and circulate the survey.

Step 4: Design the survey

Because the design of the survey has a significant influence on both the response rate and the interpretation of results, you need to ensure that the questions chosen will provide the information that is relevant to your objectives and that points to specific actions you can take following the survey to improve security culture. The survey can be conducted using either computer-based questionnaires or printed forms. The choice of method will depend on a number of considerations:

Computer-based questionnaires

> *Advantages*: Relatively fast to design and circulate to employees; analysis can be automated; outputs can be designed in advance; a larger number of questions can be included.
>
> *Disadvantages*: Difficult to persuade employees that the surveys are anonymous; many employees might not have access to computers; the surveys might be seen as a corporate survey for office-based employees rather than for workers.

Paper-based questionnaires

> *Advantages*: Can be handed to all employees as they arrive for work or from distribution points (and collected by the same method using drop-boxes); can be machine-readable so that data analysis is automated; provides anonymity.
>
> *Disadvantages*: Might be thrown away, thereby reducing the response rate; slightly higher costs associated with printing, distribution and collection; may be seen as old-fashioned.

For the remainder of this guide, we will focus on a paper version of the survey. WINS has also developed a computer–based security culture survey tool; please contact us for further information on its use and availability to organisations.

The (machine-readable) survey we describe here consists of 20 statements. Respondents are asked to indicate their level of agreement with each statement on a scale of 1 to 9 (plus an additional option of "Don't Know").

O	O	O	O	O	O	O	O	O	O
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
Strongly Disagree								*Strongly Agree*	*Don't Know*

Approximately one-third of the statements are designed so that a response of "Strongly Disagree" is a positive result. (The purpose is to help detect whether respondents simply tick "Strongly Agree" without first reading the question.)

The survey should be designed to maintain the anonymity of all personnel who complete it. However, to enable comparison of opinions and perceptions between different categories of employees, the survey should ask participants to indicate their gender, age range and general employment group; examples of employment groups include:

Senior Management Group	O
Engineering Staff	O
Safety Staff	O
Operations Staff	O
Scientific and Technical Staff	O
Security Staff	O
Business and Administration Staff	O
External Contractors	O

The statements chosen directly relate to, and can be measured against, the survey's objectives; they focus on observable behaviours rather than on thoughts and motives. Furthermore, care should be taken to ensure that employees can easily respond to and complete the statements and that trick questions are avoided. This survey will take employees approximately 20 minutes to complete. (A much longer survey would likely be counterproductive because employees could decide it takes too long to complete and simply throw it away.)

Step 5: Prepare employees to take the survey

A week before employees and contractors take the survey, an announcement should be made that a survey is going to take place. Details of the survey could be published on the organisation's website, as well as in flyers, and discussed in employee groups with line managers. The following information should be addressed:

- What security culture is and why it's important to measure it
- The audience for the survey
- When and how the survey will be conducted
- How long the survey will take
- Assurances of anonymity
- When the results will be announced
- How the results will be used
- The fact that the survey will be repeated approximately once a year

Step 6: Deliver the survey

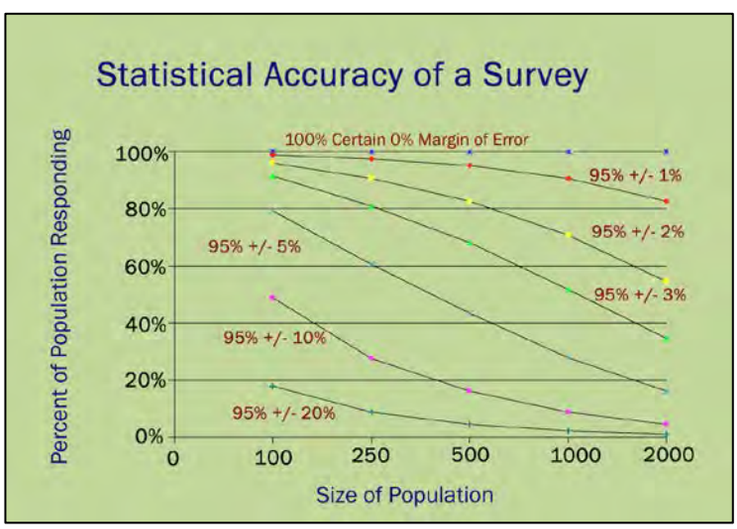
The survey design consists of a printed questionnaire (with or without a sealable envelope). It should have a unique number to identify it, but not the specific employee who filled it out. Copies should be distributed to staff and employees by hand as they arrive for work.

Employees should be asked to complete the surveys within a 48-hour period. Collection boxes need to be set up in convenient areas throughout the site. Once completed, each survey needs to be sealed in the envelope (if provided) and inserted into the collection box.

Step 7: Analyse the results

Your aim should be to complete the analysis and provide a report to senior management within four to six weeks. The validity of the survey will depend on the response rate to it; the more surveys completed, the more valid the findings. The following figures demonstrate the percentage of respondents needed to give different levels of confidence in the answers; this is a particularly important consideration if the intention is to repeat the survey at regular intervals (e.g. annually) to measure changes in attitude over time.

Respondents Needed at Error of ± 3%, ±5%, & ±10%			
Population	**± 3%,**	**±5%,**	**±10%**
500	345	220	80
1,000	525	285	90
3,000	810	350	100
5,000	910	370	100



Step 8: Brief the Senior Management

After the survey has been completed, representatives of your senior management team should receive the results first so they can begin to consider the key messages and actions that are required. They also need to plan how they will respond to less than optimum results. For example, if the survey identifies that communication is poor, senior management need to be prepared to propose a solution, such as by creating employee feedback forums and holding regular employee briefings on security.

Step 9: Brief employees on the results

Line management should brief employees face-to-face on the results of the survey within three months of its completion. During the meetings (which should last about 30 minutes), managers need to highlight the strengths and weaknesses identified through the survey; they also need to invite employees to ask questions and offer suggestions.

The following issues should be addressed in the briefing:

Areas needing improvement What needs to happen How it will happen Timescales for action Action owner (who is responsible and accountable)	Resources required Targets for improvement and measurement methods Review of dates and progress reviews, including follow-on surveys Dealing with the media and the public

Your goal should be to identify major trends and the action steps you will take to resolve them, not to over-analyse the data. It is also important to select a few key areas for action rather than to attempt to address all issues at the same time. The areas chosen should be those with maximum impact and minimum resource requirements. Furthermore, it should always be assumed that the final results will find their way into the public domain; consequently, you need to prepare a media communications plan in advance for sharing the results.

Step 10: Repeat the Survey

To determine whether the security culture changes over time, conduct the survey on an annual basis.

Choosing the Questions for the Survey

The questions you choose for the survey will depend on a range of factors, such as the objectives, resources available, and size and complexity of the organisation. As noted earlier, it is important that the objectives be considered carefully and that the questions be appropriate to the audience; there is little point asking general employees whether they think the oversight arrangements implemented by the board of directors are effective because they are unlikely to have any personal experience of this.

Organisations like the IAEA and INPO have published extensive guidance on assessing attitudes to safety culture, but it is only now that attention is turning to the issue of security culture. Nevertheless, the published guidance on safety culture provides a solid foundation on which to develop questions for a security attitude survey.

The nine traits that INPO identifies are:

- Questioning attitude
- Continuous learning
- Effective safety communication
- Problem identification and resolution
- Leadership safety values and actions
- Environment for raising concerns
- Decision-making
- Work processes
- Respectful work environment

In the tables that follow, we have summarised the key features of INPO's guidance on safety culture and the associated traits. We have then chosen 20 questions that reflect these key aspects, focusing on topics that are most relevant to employees, and mapped them to both the INPO guidance and the factors identified in this Best Practice Guide. In this way it is possible to understand how the questions were selected, what they tell you about an organisation, and how you can increase the number of questions if you feel you need a larger survey.

TABLE 1: INPO 12-012: TRAITS OF A HEALTHY NUCLEAR SAFETY CULTURE		
TRAITS	**TRAIT DEFINITION**	**ATTRIBUTES (SUMMARISED)**
Personal accountability	All individuals take personal responsibility for safety.	• Safety standards are adhered to individually and collectively. • Individuals understand their accountability for safety, willingly raise their concerns, encourage teamwork, and have a strong sense of collaboration and cooperation where safety is concerned.
Questioning attitude	Individuals avoid complacency and continuously challenge existing conditions and activities to identify discrepancies that might result in error or inappropriate action.	• Nuclear technology and materials are recognised as being special in relation to all aspects of safety. • Individuals stop work or challenge any situation where risks to safety or unexpected conditions are experienced. • Individuals challenge assumptions and offer opposing views when they think something relating to safety is not correct. • Complacency is avoided at all times in relation to nuclear safety. Both the organisation and individuals recognise and plan for the possibility of mistakes, latent problems and inherent risks, even while expecting successful outcomes.
Effective safety communication	Communications maintain a focus on safety.	• Communications within and between workgroups are timely, frequent and accurate so that everyone has the information necessary to accomplish work activities safely and effectively. • Individuals provide complete, accurate and forthright information to oversight, audit and regulatory organisations. • Leaders promptly communicate expected outcomes, potential problems, and planned contingencies. Furthermore, they periodically verify that the information has been understood by teams and individuals. • Executives and senior managers reinforce the importance of nuclear safety by clearly communicating its relationship to strategic issues, including budget, workforce planning, equipment reliability, business plans and behaviours. • Leaders encourage the free flow of information and are responsive to feedback. They understand that the upward flow of information in the organisation is just as important as the downward flow of information.

TRAITS	TRAIT DEFINITION	ATTRIBUTES (SUMMARISED)
Leadership safety values and actions	Leaders demonstrate a commitment to safety in their decisions and behaviours.	• Executive and senior managers are the leading advocates of nuclear safety and demonstrate their commitment both in word and action. The nuclear safety message is communicated frequently and consistently, occasionally as a standalone theme. Leaders throughout the nuclear organisation set an example for safety period corporate policies and emphasise the overriding importance of nuclear safety. • Executives and senior managers ensure that there are adequate staffing levels to maintain safety, personnel are suitably qualified, and that all other necessary resources are provided to ensure a safe operating environment, including risk management tools and emergency equipment. • Managers and supervisors are visibly present in the field and provide coaching, mentoring and other leadership activities to reinforce standards and positive decision-making practices and behaviours in relation to safety. • Leaders publicly praise behaviours that reflect a positive safety culture and managers reward individuals who identify and raise issues that affect nuclear safety. The environment promotes accountability and holds individuals accountable for their actions. • Executives and senior managers ensure corporate priorities. Strategic and business plans are aligned with nuclear safety and use information from independent oversight organisations to establish priorities that align with nuclear safety. • Leaders use a systematic process for evaluating and implementing change so that nuclear safety remains the overriding priority. For example, changes to organisational structure and function, leadership, policies, programmes, procedures and resources should be assessed for their impact on safety and action taken to avoid any negative consequences. • Executives and senior managers obtain outside perspectives on nuclear safety from qualified, independent organisations and personnel, and also use a variety of monitoring tools including employees surveys, self-assessments and external feedback to assess nuclear safety culture. • Leaders encourage personnel to challenge unsafe behaviour and unsafe conditions, and they support personnel when they need to stop plant operations and activities for safety reasons. • Leaders maintain high standards of personal conduct that promote a positive nuclear safety culture, actively seek out the opinions and concerns of workers at all levels, and act promptly when a nucleus safety issue is raised to ensure it is understood and appropriately addressed.

TRAITS	TRAIT DEFINITION	ATTRIBUTES (SUMMARISED)
Decision-making	Decisions that support or affect nuclear safety are systematic, rigorous and thorough.	• Senior leaders support and reinforce conservative decisions. • Leaders seek input from different work groups or organisations as appropriate when making safety or risk-significant decisions. • Leaders take a conservative approach to decision-making, particularly when information is incomplete or conditions are unusual. • The onsite licensed operators have the authority and responsibility to place the plant in a safe condition when faced with expected or uncertain conditions. • The organisation ensures that important nuclear safety decisions are made by the correct person at the lowest appropriate level.
Respectful work environment	Trust and respect permeate the organisation.	• The organisation regards individuals and their professional capabilities and experience as its most valuable asset. • Individuals at all levels of the organisation treat each other with dignity and respect and do not demonstrate or tolerate bullying or humiliating behaviours. • The organisation and its leaders encourage individuals to offer ideas, concerns, suggestions, differing opinions and questions to help identify and solve problems. • Individuals value the insights of the perspectives provided by quality assurance, the employee concerns program, and independent oversight organisation personnel. • Individuals have confidence in the organisation that conflicts will be resolved respectfully and professionally, in a balanced, equitable and consistent manner.

TRAITS	TRAIT DEFINITION	ATTRIBUTES (SUMMARISED)
Continuous learning	Opportunities to learn about ways to ensure safety are sought out and implemented.	• The organisation systematically and effectively collects, evaluates and implements relevant internal and external operating experience in a timely manner. • Operating experience is used to understand equipment, operational and industry challenges, as well as to adopt new ideas to improve performance. • Independent and self-assessments, including nuclear safety culture assessments, are thorough and effective and used as a basis for improvement. • Self-assessments are performed at a regular frequency. Self-assessment teams include individual contributors and leaders from within the organisation and from external organisations when appropriate. • The organisation participates in benchmarking activities, seeks out best practices, and makes adjustments to improve performance. • The organisation provides training that ensures knowledge transfer to maintain a knowledgeable, technically competent workforce. • Leadership and management skills are systematically developed, and executives obtain the training necessary to understand basic plant operations and the relationships between major functions and organisations.
Problem identification and resolution	Issues potentially impacting safety are promptly identified, fully evaluated and promptly addressed and corrected commensurate with their significance.	• The organisation implements the corrective action program with a low threshold for identifying issues. Individuals identify and report issues completely, accurately and in a timely manner in accordance with the programme. • The organisation thoroughly evaluates problems to ensure that their resolution addresses root causes to identify and correct the fundamental cause of significant issues. • Trends in safety performance indicators are acted on to resolve problems early. • The organisation develops indicators that monitor both equipment and organisational performance, including safety culture.

TRAITS	TRAIT DEFINITION	ATTRIBUTES (SUMMARISED)
Environment for raising concerns	A safety conscious work environment is maintained where personnel feel free to raise safety concerns without fear of retaliation, intimidation, harassment or discrimination.	• The organisation effectively implements policies that support individuals' rights and responsibilities to raise safety concerns and does not tolerate harassment, intimidation, retaliation or discrimination for doing so. • The organisation effectively implements a process for raising and resolving concerns that is independent of line management influence. Safety issues may be raised in confidence and are resolved in a timely and effective manner. • Individuals assigned to respond to concerns have the appropriate competences.
Work processes	The process of planning and controlling work activities is implemented so that safety is maintained.	• Work management is a deliberate process in which work is identified, selected, planned, scheduled, executed, closed and critiqued. The entire organisation is involved in and fully supports the process. • Work activities are coordinated to address conflicting or changing priorities across the whole spectrum of activities contributing to nuclear safety. • The work process supports nuclear safety and maintenance of design margins by minimizing long-standing equipment issues, preventive maintenance deferrals, and maintenance and engineering backlogs. • The organisation creates and maintains complete, accurate and up-to-date documentation. • Individuals review procedures and instructions prior to work to validate they are appropriate for the scope of work and that required changes are completed prior to implementation.

WINS EMPLOYEE SECURITY ATTITUDE SURVEY: RELATIONSHIP TO INPO TRAITS AND BPG ELEMENTS		
INPO TRAIT	**WINS BPG ELEMENT**	**SURVEY QUESTIONS**
Leadership security values and actions	Organisational Leadership Strategic context	1. Senior management think that security is important.
Leadership security values and actions	Organisational Leadership Strategic context	2. Senior management think that nuclear security and safety are equally important.
Effective security communication	Employee engagement	3. I have not been informed about the main security threats we could experience here.
Effective security communication	Organisational Management Systems Employee Engagement	4. The security policies and procedures that affect me are clear and well communicated.
Personal accountability Effective security communication	Organisational Management Systems	5. I do not fully understand the security requirements with which I am expected to comply.
Continuous learning	Employee Engagement	6. The training I have received on security is clear and comprehensive.
Effective security communication Environment for raising concerns	Employee Engagement	7. I am encouraged to provide feedback and comments on my views of the security arrangements.
Personal accountability Questioning attitude	Organisational Leadership	8. My managers sometimes expect me to take shortcuts that do not comply with the security arrangements.
Questioning attitude	Comprehensiveness of the Security Programme	9. I do not feel confident about the security arrangements on this site.
Personal accountability	Employee Engagement	10. Good security helps protect my job and my safety, and I support it.
Environment for raising concerns Respectful work environment	Employee Engagement	11. If I were to become aware of security issues that concern me, I would report them even if they involved a work colleague.

WINS EMPLOYEE SECURITY ATTITUDE SURVEY: RELATIONSHIP TO INPO TRAITS AND BPG ELEMENTS		
INPO TRAIT	**WINS BPG ELEMENT**	**SURVEY QUESTIONS**
Environment for raising concerns	Employee Engagement	12. I know how to report security concerns using our organisation's whistle-blower system.
Questioning attitude Environment for raising concerns	Comprehensiveness of the Security Programme	13. Security should be improved on this site; attitudes to security are complacent.
Respectful work environment	Comprehensiveness of the Security Programme	14. The people who work in the Security Department are highly professional.
Decision making Respectful work environment	Comprehensiveness of the Security Programme	15. I am confident that the security systems and guards would manage a security threat in an effective way.
Decision making Respectful work environment	Comprehensiveness of the Security Programme	16. The search procedures on the way into the site are very thorough.
Decision making	Comprehensiveness of the Security Programme	17. It would be easy to steal things from this site undetected.
Leadership security values and actions	Organisational Leadership	18. Senior management visibly promote the importance of security in the workplace.
Effective security communication	Employee Engagement	19. The way that security requirements are communicated to staff is poor.
Effective security communication Respectful work environment	Employee Engagement	20. I have the opportunity to discuss security arrangements at the staff meetings I attend.
		Any additional comments or remarks you would like to make?

APPENDIX B:

Security Culture Maturity Scale

The following scale presents five stages of development leading to a world-class nuclear security culture, each with its own set of characteristics. Identifying where your organisation falls on this scale will help you understand how effective your security culture is and what you need to do to improve it.

LEVEL	CHARACTERISTICS
1 WORLD CLASS	Leadership has defined and documented a comprehensive Security Policy that is overseen by the Board of Directors and sets organisational expectations and requirements. The maintenance of an effective, performance-based, performance-tested security programme is seen as a core company value. Leading indicators for security preparedness are used extensively throughout the organisation. There is no sense of security complacency in any part of the organisation. All staff give security the same high priority they give nuclear safety. All employees share the belief that security is a critical aspect of their job and that they share responsibility for preventing security incidents. Employee engagement is excellent, with multiple opportunities for feedback and learning from experience.
2 HIGHLY EFFECTIVE	The majority of staff in the organisation believe that security is important. Therefore, they lead by example. Managers and frontline staff understand that security vulnerabilities can be caused by a variety of events and that managerial behaviour needs to constantly reinforce the importance of effective security arrangements. Frontline staff accept personal responsibility for security and take appropriate action when security weaknesses are identified. The organisation puts significant effort into proactive measures to prevent security weaknesses, including employee engagement and the testing of arrangements. Security performance is measured using all data available, including leading indicators.

3 GOOD	Security is recognised as an important business risk and is overseen by a senior management committee. The organisation believes that security threats are real and that staff at all levels should be involved in helping to achieve an effective security culture. The Security Programme is understood and endorsed by the organisation's senior management. The majority of staff are prepared to support the security objectives and to take personal responsibility for their own security and those around them. Employee engagement is developing, and security briefings allow feedback from staff. Security performance is monitored, and some leading security indicators are being used.
4 DEVELOPING	Security is seen in terms of regulatory compliance and the adherence to rules and procedures that have been set by the regulator. Security is reluctantly seen as a business risk; senior management view it as an unavoidable financial overhead and believe the risk of an incident is extremely small. The Security Department owns the security programme and provides only general, periodic reports to senior management. Employee engagement is limited to periodic briefings about security rules. Security performance is measured by lagging indicators, such as the number of occasions when the regulator has identified security non-compliances. Senior managers are reactive to their involvement in security. Staff comply with security rules, but they consider them to be intrusive.
5 INEFFECTIVE	Security is defined and thought about only in terms of compliance with regulations at minimum cost. Security is not seen as a key business risk, and the postulated threats are not considered to be real. Security is seen as the sole responsibility of the Security Department and/or guard force. Excessive and unnecessary secrecy prevent employee engagement with the security arrangements. Security violations and shortcuts in procedures are not considered serious. Most frontline staff are uninterested in security and see it as an obstacle to getting their work done.

WINS Best Practice Guides

Group 1: Nuclear Security Programme Organisation

1.1 Effective Security Regulation and Implementation
1.2 Legal Accountability and Liability for Nuclear Security
1.3 Security Governance
1.4 Nuclear Security Culture
1.5 Security Performance Metrics
1.6 Making Security Efficient

Group 2: Managing and Communicating Security Information

2.1 Threat Assessment
2.2 Managing Security Threat Information
2.3 Information Security for Operators: Challenges and Opportunities
2.4 Communicating Security Information: Striking a Balance
2.5 Engaging with External Stakeholders on Nuclear Security

Group 3: People in Nuclear Security

3.1 Developing Competency Frameworks for Personnel and Managment with Accountabilities for Nuclear Security
3.2 Human Reliability as a Factor in Nuclear Security
3.3 Nuclear Security for Scientists and Engineers
3.4 Managing Internal Threats
3.5 Working Effectively with External Response Forces
3.6 Nuclear Security Guard Recruitment and Selection
3.7 Guard Force Training and Motivation
3.8 Effective Management and Deployment of Armed Guard Forces

Group 4: Implementing Security Measures

4.1 Security by Design
4.2 An Integrated Approach to Nuclear Safety and Nuclear Security
4.3 Security of IT and IC Systems at Nuclear Facilities
4.4 Nuclear Material Accountancy and Control in Support of Nuclear Security
4.5 Learning from Operating Experience
4.6 Security Exercises
4.7 Modelling and Simulation for Nuclear Security
4.8 Electronic Tracking for the Transport of Nuclear and other Radioactive Materials
4.9 Security Equipment Maintenance
4.10 Nuclear Transport Security
4.11 Effectively Integrating Physical and Cyber Security
4.12 Security of Dry Storage of Spent Nuclear Fuel

Group 5: Security of Radioactive Sources

5.1 Security of High Activity Radioactive Sources
5.2 Security of Well Logging Radioactive Sources
5.3 Security of Industrial Radiography Sources
5.4 Security of Radioactive Sources Used in Medical Applications
5.5 Security Management of Disused Radioactive Sources

WINS**ACADEMY**

Security threats are becoming more complex, security is becoming more expensive to implement, and the nuclear industry is facing growing economic pressures. Certified professional training and sharing of operational experience has been shown to improve safety and reactor performance; and in the same way, many States and organisations believe that certified professional training lies at the heart of operational excellence for security. Now, for the first time, personnel with management accountabilities for nuclear security can receive certification through the WINS Academy and enhance their personal and organisational competitiveness.

All WINS Academy participants take a core Foundation Module and then choose an Elective Module dependent on the participant's area of responsibility. We offer Elective Modules for:

Nuclear Security Governance
Nuclear Security for Scientists, Technicians and Engineers
Nuclear Security for Executive Managers
Radioactive Source Security Management
Nuclear Security Incident Management
Nuclear Security Progamme Management
Nulcear Security Regulation
Communicating with Civil Society
Transportation Security Management

For further information on the WINS Academy and WINS Best Practice Guides please go to WINS website **www.wins.org**

ISBN: 978-3-903031-80-7

Tel.: +43 1 23060 6083 | Fax: +43 1 23060 6089 | Email: info@wins.org | Internet: www.wins.org
International NGO under the Austrian Law BGBI. Nr. 174/1992 | GZ: BMeiA-N9.8.19.12/0017-I.1/2010