Nuclear Industry

Safety Directors' Forum

Issue 1
June 2013

KEY ATTRIBUTES OF AN Excellent Nuclear Security Culture

Produced in Association With

Department of Energy & Climate Change

The National Skills Academy NUCLEAR

Office for Nuclear Regulation
An agency of HSE

FOREWORD

On behalf of the UK Nuclear Industry Safety Directors Forum, the Office for Nuclear Regulation, and the Department of Energy and Climate Change, we very much welcome this short guide on civil nuclear security culture.

The move to NORMS and goal setting means that it is no longer enough to just follow the rules – we can all make a difference and enhance security effectiveness if we understand the rationale and importance of security measures and own the outcomes that we seek to achieve.

The attitude, behaviour and actions (or culture) of those in leadership, management, implementation and compliance positions will be critical which is why the excellent guidance contained in this leaflet is so crucial particularly as it applies across the industry, regulators and industry.

Together we can ensure that the UK Civil Nuclear Industry has a proportionate, risk based response to security challenges in the same way as we have to Nuclear Safety

Finally we would like to hold up the development of this guidance as a fine example of tripartite working which has produced very simple and helpful guidance.

AR Brandwood,

A R Brandwood,
Chair UK Nuclear Industry Safety Directors Forum

A R Freer,
Deputy Chief Nuclear Inspector (Civil Nuclear Security),
Office for Nuclear Regulation.

S Murphy
Acting Director for Nuclear Resilience & Assurance Directorate

Introduction

Adrian Freer, Deputy Chief Inspector Civil Nuclear Security (CNS) gave a presentation on the 'new approach' to security regulation during the March 2012 Safety Directors Forum, (SDF). As a result, a tripartate security sub group was established including representatives of the Office for Nuclear Regulation (ONR) and the Department for Energy and Climate Change (DECC), under direction of the Safety Directors Forum (SDF). One of this group's first undertakings was to develop a better understanding of the attributes of an excellent nuclear security culture, and for this to be captured and codified.

This short guide has been developed specifically for the key stakeholders associated with the delivery of UK civil nuclear security. It is intended to assist those who are charged with setting the vision for the nuclear security culture needed to ensure the successful achievement of security objectives associated with outcome-based regulation. Those objectives and associated requirements are contained in respective framework documents, such as the National Objectives, Requirements and Model Standards (NORMS) document and ONR Security Policy Framework (SPF) document.

The following guidance should be read in conjunction with other relevant guidance such as that from the Institute of Nuclear Power Operators, (INPO), the International Atomic Energy Agency (IAEA) and World Institute for Nuclear Security (WINS).

Key Attributes

Detailed in the guidance are eight key attributes, identified as part of the development process for the civil nuclear industry. All are essential for the security culture required and each attribute lists what is required of:

A. Government (in particular DECC. Other Government Departments (Home Office, Cabinet Office) will have a role to play also)

B. ONR

C. Companies and Organisations

D. Senior Management and employees including contractors and consultants

The eight key attributes of an excellent Civil Nuclear Security Culture are summarised below and detailed in Annexes A to H.

A. A risk driven security programme which takes due consideration of proportionality

B. Competent, capable and sufficient security resources

C. Security performance is monitored at all levels in the organisations as appropriate – board level to delivery team

D. An appropriate, independent governance regime led by the Board

E. All employees understand the security risks and consequences appropriate to their role and their part in managing and mitigating risks

F. Security expectations and standards are set, communicated and understood. All are held accountable with regards to compliance

G. Learning and performance process for security are in place and the organisations security performance is continually improving

H. All employees are engaged in security matters as appropriate and their views on security are carefully considered

Key Behaviours

Senior management can use the guidance in this document in each of the eight attributes to conduct a gap analysis of their organisational and employee civil nuclear security culture, with the aim of where necessary developing an appropriate improvement programme. Some key behaviours that apply to the key attributes are detailed below:

A. The adoption of a risk based approach to the management of civil nuclear security and use of similar processes to those used for managing other business/ organisational risks

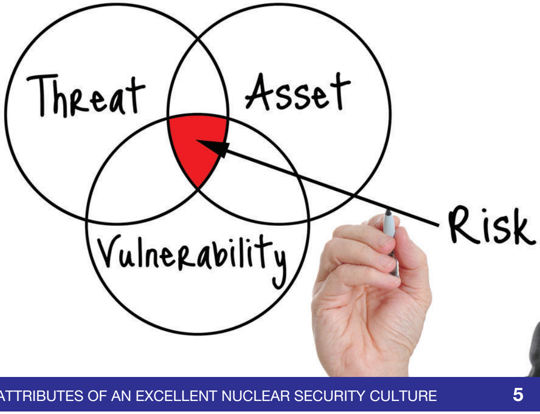
B. The behaviours required for a successful implementation of NORMS and SPF requirements should consider alignment into the HR processes of DECC, ONR and the regulated Companies and Organisations, especially with regard to selection, training, development, performance management

C. The adoption of a learning approach including consideration of the lessons of how the industry moved to goal setting nuclear safety

D. Setting the right expectations for an effective security culture at every level (i.e. within DECC, ONR, and those Companies and Organisations subject to regulation) is critical. All these expectations must be aligned and the guidance in this document should assist this process

E. Appropriate monitoring of overall civil nuclear security performance and the effect of improvement programmes at every level is essential, including at the most senior levels

F. Being as open as security arrangements will allow with all involved in maintaining civil nuclear security standards, so as many persons as possible can understand the highest levels of compliance that should be achieved



ANNEX A - A RISK DRIVEN SECURITY PROGRAMME

GOVERNMENT

1. DECC should specify its 'risk appetite' in respect of civil nuclear security This should, where possible, be proportionate and clear in relation to the threat to Nuclear Material (NM), Other Radioactive Material (ORM) (including radioactive sources) and Sensitive Nuclear Information (SNI), and consistent with the Nuclear Industries Security Regulations (NISR 2003) as amended. As part of this process DECC should:

a. Consult with Industry and ONR on the threat.

b. Clearly define which risks (resulting from security issues) are the responsibility of which bodies, e.g. reputational.

c. Facilitate a clear understanding across all relevant stakeholders of threats/risks.

ONR

2. ONR has a responsibility to lead by example, as part of enabling a risk driven security programme it should:

a. Facilitate and assure that there is a clear understanding across all relevant stakeholders of threats/risks;

b. Ensure regulation is aligned with agreed risks and is proportionate; and

c. Ensure that CNS Inspectors are selected and trained as required to regulate in this way.

COMPANIES AND ORGANISATIONS

3. Companies and Organisations should have in place a nuclear security policy statement that declares a sound commitment to quality of performance in all nuclear security activities. As part of this process they should:

a. Have in place an effective security risk process that feeds into the corporate risk process;

b. Accept threat as a baseline for site security and proportionate in the site security case;

c. Ensure the company/organisation and it's employees understand the security threat and risks; and

d. Engage at all levels on security issues (as with EHSQ).

PERSONAL

4. All personnel should understand their part in ensuring security threats are controlled and managed and all Board members and senior executives and managers should take leadership roles with regards to security as they do with EHSQ.

ANNEX B - COMPETENT, CAPABLE, SUFFICIENT SECURITY RESOURCES

GOVERNMENT

1. DECC should ensure, where possible, that HMG security responsibilities are funded and properly resourced (e.g. the Civil Nuclear Constabulary (CNC), Nuclear Decommissioning Authority (NDA) etc), recognising that there are a number of factors that will affect this including proportionality and value for money considerations and that:

a. Attempt to ensure there is policy consistency to allow ONR, Industry, etc to plan, recognising that there are factors that may affect this, for example changes in government ministers; and

b. security accountabilities are clear, e.g. who is responsible for site physical security.

ONR

2. ONR should ensure that the delivery of its regulation is delivered or facilitated by specialists . ONR should also ensure inspectors understand the impact of their decisions on organisations and this understanding informs their judgements and decisions.

COMPANIES AND ORGANISATIONS

3. Companies and Organisations should set security competence standards and build them into HR processes. They should also ensure:

a. Competence on company Boards with regards to security; and

b. Have ownership control of security resources to enable responsibilities to be carried out.

PERSONAL

4. Take on the obligations on individual’s responsibility for security in the same way as EHSQ.

Virus Alert!
Warning! Threat detected!
A malicious item has been detected!

ANNEX C - SECURITY PERFORMANCE MEASURED AT ALL LEVELS IN THE ORGANISATION AS APPROPRIATE – BOARD LEVEL TO DELIVERY TEAM

GOVERNMENT

1. DECC should be clear on thetype of information and level of assurance and analysis required by ministers; and interpret performance information intelligently.

ONR

2. ONR should promote continuous improvement (consistent with outcome based/goal setting regime) and:

a. Support the development of a KPI framework and the setting of performance objectives;
b. Take a considered view of performance and provide balanced feedback;
c. Adjust scrutiny accordingly (i.e. provide targeted resource to regulate poor performance);
d. Assure Government; and
e. Set a positive example.

COMPANIES AND ORGANISATIONS

3. Companies and Organisations should Identify areas of performance for improvement (or to sustain excellent performance and:

a. Develop KPI framework and establish appropriate indicators appropriate for business;
b. Set targets for improvement;
c. Communicate expectations to workforce;
d. Monitor and report performance to Executive; to be overseen by Board;
e. Have ‘independent challenge’ in place; and
f. Bench-mark performance periodically and work collaboratively with other organisations in supporting the development of industry good practice

PERSONAL

4. All personnel should understand security performance and expectations, participate in improvement activities and report events and matters in accordance with NISR 2003.

ANNEX D - AN APPROPRIATE, INDEPENDENT GOVERNANCE REGIME LED BY THE BOARD

GOVERNMENT/ONR/COMPANIES AND ORGANISATIONS

1. All the above are to ensure that appropriate (i.e. effective and proportionate) information and advice is available for all appropriate levels with the breadth of competence to interpret it and:

a. Set actions accordingly and monitor delivery;

b. Ensure that each body/organisation has their own nuclear security risk register and act on mitigation actions and feed significant risks main ‘company/ risk register; and

c. Ensure organisational management systems are in place where arrangements ensure that correct information is fed into the governance processes.

PERSONAL

2. Individuals should be confident about how a ‘whistle blowing’ process operates and be able to access evidence that shows a fair reporting culture.

ANNEX E - ALL EMPLOYEES UNDERSTAND THE SECURITY RISKS AND CONSEQUENCES PROPRIATE TO THEIR ROLE AND THEIR PART IN MANAGING AND MITIGATING RISKS

GOVERNMENT

1. DECC should ensure effective intelligence architecture is in place and that:

a. A strategy for effective dissemination of intelligence information exists; and

b. All individuals are capable of being briefed to the full extent of their security clearance.

ONR

2. ONR should support the delivery of information on the threat, in context, to the industry and ensure that there is an appropriate and sufficient understanding of threat information throughout the industry.

COMPANIES AND ORGANISATIONS

3. Companies and Organisations should have systems, processes and competence to deliver threat information to all employees tailored to their security clearance and their role. They should also have an effective security risk register and system for communicating of risks; these risks should also feed into training and development.

PERSONAL

4. All personnel should use security information responsibly to:

a. manage/mitigate;

b. improve performance; and

c. understand the consequence of misuse.

ANNEX F - SECURITY EXPECTATIONS AND STANDARDS ARE SET, COMMUNICATED AND UNDERSTOOD. ALL ARE HELD ACCOUNTABLE WITH REGARDS TO COMPLIANCE

GOVERNMENT

1. DECC should set and explain the strategic objectives/expectations, seek evidence from industry through ONR that these are being achieved and intelligently interpret information.

ONR

2. ONR should develop and deliver the security objectives to be achieved and identify appropriate good practice, commission work to fill voids and support development thereof. ONR should also:

a. Explain the rationale for expectations;
b. Explain the methodologies for assessment;
c. Align interventions to achievement of objectives;
d. Deliver appropriate proportionate enforcement when necessary; and
e. Advise DECC on appropriateness of its expectations.

COMPANIES AND ORGANISATIONS

3. Companies and Organisations should have a system of self-assessment in place to maintain motivation, leadership, and security culture in general. As part of this process, they should also:

a. Promote security responsibility from board and executive level;
b. Integrate security expectations into normal business;
c. Translate objectives and good practice into local policy and procedures;
d. Provides resource to enable communication of expectations;
e. Communicate expectations to workforce; check understanding;
f. Have a proactive and reactive ability to ensure individual accountability;
g. Use internal and external resources to review success of initiatives; and have an 'independent challenge' in place;
h. Take action against individuals when appropriate (rehabilitation as well as punishment);
i. Communicate to show that transgressors have been dealt with;
j. Monitor and report performance to Exec; to be overseen by Board;
k. Bench-mark performance periodically and work collaboratively with other companies and organisations in supporting the development of industry good practice; and
l. Have a 'whistleblower' policy in place.

PERSONAL

4. All personnel should understand security expectations and strive to achieve standards. They should also participate in improvement activities, encourage others and report events and matters in accordance with NISR 2003.

ANNEX G - LEARNING AND DEVELOPMENT – CONTRIBUTION TO EXCELLENT SECURITY CULTURE

GOVERNMENT

1. DECC should ensure that there is an appropriate legislative and policy framework in place.

ONR

2. ONR should assist industry in turning legislative high-level requirement(s) into goals to be achieved by industry and in the development of security learning content. ONR should also:

a. Promote continuous improvement (consistent with outcome based/goal setting regime);
b. Support the development by industry of a security competency framework and the setting of appropriate security L&D performance objectives;
c. Take a considered view of security L&D performance and provide balanced feedback;
d. Provide proportionate regulation prioritised to target poorest performers first;
e. Assure Government.

COMPANIES AND ORGANISATIONS

3. Companies and Organisations should identify areas of security L&D performance for improvement (or to sustain excellent performance) in order to meet objectives/goals. They should also:

a. Set targets for security L&D improvement;
b. Develop competency framework and establish appropriate performance indicators;
c. Communicate security L&D expectations to the workforce;
d. Monitor and report performance to Chief Exec; to be overseen by Board;
e. Bench-mark security L&D performance periodically and work collaboratively with other companies/organisations in supporting the development of industry good practice;
f. Provide an environment where personnel feel empowered to challenge security behaviours in others; and
g. Provide realistic and effective training and development opportunities for staff in security matters.

PERSONAL

4. All personnel have a responsibly to constructively challenge security behaviours in others when appropriate and to:

a. Report events and matters in accordance with NISR 2003;
b. Participate in security training and learning activities; and
c. Put security learning into practice.

ANNEX H - ALL EMPLOYEES ARE ENGAGED IN SECURITY MATTERS AS APPROPRIATE AND THEIR VIEWS ON SECURITY ARE CAREFULLY MEASURED

GOVERNMENT

1. DECC should enable engagement by being clear on what information can be shared (i.e. people need to be 'in the know' to be fully engaged) within the boundaries of legislative requirements .

ONR

2. ONR should ensure that it's own staff are able to explain the importance of security. ONR should also:

a. Survey views periodically on the effectiveness of sharing arrangements for security information ;

b. Involve the industry in developing improvements; and

c. Support companies and organisations through intervention activities that seek and assess evidence of engagement and support the development of local initiatives.

COMPANIES AND ORGANISATIONS

3. Companies and Organisations should explain the importance of security to staff in the context of its own organisational activities and identify training needs (i.e. what, why, who, when). They should also:

a. Provide training, monitor effectiveness and periodically refresh, as required;

b. Survey views periodically and consult internally on changes;

c. Involve its staff in developing improvements; and

d. Provide evidence of engagement to ONR (i.e. by survey/audit).

PERSONAL

4. All personnel should understand the requirements, do as trained, and be involved in improvement initiatives. They should also adopt a questioning and challenging approach; be vigilant and report events and matters in accordance with NISR 2003.

LIST OF ABBREVIATIONS

CNC	Civil Nuclear Constabulary
DECC	Department for Energy and Climate Change
EHSQ	Environmental Health, Safety and Quality
HMG	Her Majesty's Government
HR	Human Resources
IAEA	International Atomic Energy Agency
INPO	Institute of Nuclear Power Operators
KPI	Key Point Indicator
L&D	Learning and Development
NDA	Nuclear Decommissioning Authority
NISR	Nuclear Industries Security Regulations
NORMS	National Objectives, Requirements and Model Standards
NM	Nuclear Material
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
SDF	Safety Directors Forum
SLC	Site Licence Company
WINS	World Institute for Nuclear Security

Page left intentionally blank for note purposes

SECURITY
SECURITY