The Threat			
Doc. Type	ONR Technical Assessment Guide (TAG)		
Unique Doc. ID:	CNS-TAST-GD-11.4.2	**Issue No.:**	1
Record Reference:	2022/16592		
Date Issued:	Apr-22	**Next Major Review Date:**	Apr-27
Prepared by:		Security Inspector Security Inspector	
Approved by:		Superintending Inspector	
Professional Lead:		Superintending Inspector	
Revision Commentary:	First Edition		

Table of Contents

1. Introduction

1. ONR has established its assessment principles, which apply to the assessment by ONR specialist inspectors of safety, security and safeguards submissions for nuclear facilities or transports that may be operated by potential licensees, existing licensees, or other dutyholders. These assessment principles are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions against all legal provisions applicable for assessment activities. This technical assessment guide (TAG) is one of these guides.

2. The term 'security plan' is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. Dutyholders under Regulation 22 of the Nuclear Industries Security Regulations 2003 ('NISR 2003') [1] may also use the ONRs Security Assessment Principles (SyAPs) [2] as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This TAG is such a guide.

2. Purpose and Scope

3. There is growing regulatory emphasis on threat reporting. Government regulations are increasingly emphasizing the requirement for organisations to use threat reporting to support risk management. This TAG contains guidance to advise and inform ONR inspectors in the exercise of their regulatory judgment during intervention activities relating to the assessment of Key Security Plan Principle (KSyPP) 2 – The Threat. Protection systems should be designed, evaluated and tested using the state's Design Basis Threat (DBT), whilst emergent threats which may not be captured in a timely manner within periodic reports or represented in the DBT should be identified through Threat Intelligence (TI) management. The TAG aims to provide general advice and guidance to ONR inspectors on how to assess this aspect of a dutyholder's security arrangements. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, or methodologies for dutyholders to follow to demonstrate they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail within their submission and for ONR to assess whether the arrangements are adequate.

3. Relationship to Relevant UK Legislation and Policy

4. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.

5. NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved security plan in accordance with Regulation 4. This regulation includes a requirement to ensure the security of equipment and software used in connection with activities involving Nuclear Material (NM) or Other Radioactive Material (ORM). NISR further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers CS&IA to be an important component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.

6. NISR 2003, together with The Energy Act (TEA) 2013 and regulatory guidance inclusive of SyAPs, assist the UK in complying with its legal obligations under the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 3). The DBT is produced and owned by HMG because it states the threat actor capabilities above which the government is prepared to take primary responsibility for defeating. Threats at or below this level of capability are the responsibility of the dutyholder to defeat and therefore are essential to underpin the design and evaluation of physical protection systems. In light of this, whilst the requirement to apply the DBT is not found explicitly in UK statutory law, its application in Vital Area Identification (VAI) studies and vulnerability assessments is considered a prerequisite of security plan approval. In that regard, its use is an integral part of dutyholders being able to demonstrate compliance with NISR.

7. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating that they have effective processes in place to achieve KSyPP 2 – The Threat. The TAG is consistent with other TAGs, associated guidance and policy documentation.

8. The Government Functional Standard on security [3] describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm’s length bodies or their contracted third parties. The security principles, governance, life cycle and practices detailed within

Functional Standard have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not.

9. The Government Security Classifications document, together with the ONR Classification Policy [4] describes types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

10. The National Cyber Security Centre (NCSC) Cyber Assessment Framework [5] states 'a good understanding of the threat landscape and the vulnerabilities that may be exploited is essential to effectively identify and manage risks', and this is key in developing effective Cyber Protection Systems (CPS) which are, according to FSyP 7 'capable of deterring, detecting, defending / defeating disruptive challenges (such as cyber-attacks)' whilst Security Delivery Principle (SyDP) 7.1 determines that 'dutyholders should ensure that they have a mature understanding of the cyber security and information risks throughout their organisation, and the lifecycle of their activities, informed by the National Technical Authority and current threat intelligence (provided by HMG and other sources)'.

4. Relationship to International Standards and Guidance

11. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [6] and the International Atomic Energy Agency (IAEA) Nuclear Security Fundamentals [7]. Further guidance is available within IAEA Technical Guidance and Implementing Guides.

12. Fundamental Principle G of the CPPNM concerns threat and specifies that physical protection should be based on the State's current evaluation of the threat. Fundamental Principle H concerning the graded approach is also of relevance and states that physical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the nuclear material and potential consequences associated with the unauthorised removal of nuclear material and with the sabotage against nuclear material or nuclear facilities.

13. The IAEA Nuclear Security Series (NSS) Fundamentals-level publication [7] and other publications in the IAEA NSS, reinforces the importance of threat information in Essential Element 7: Identification and Assessment of Nuclear Security Threats; Essential Element 8: Identification and Assessment of Targets and Potential Consequences; and Essential Element 9: Use of Risk Informed Approaches.

14. Additionally, the recommendations-level NSS publications 'Nuclear Security Recommendations on Radioactive Material and Associated Facilities' [8] and 'Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities' [9], amplify that States should define nuclear security requirements for nuclear or other radioactive material and associated facilities based on a threat assessment or a DBT; 'the competent authorities should regularly review the national threat assessment and the DBTs and revise them as needed….new or emerging threats may require immediate consideration and actions before DBTs can be revised' [10]. NSS 13 [9] specifically defines the DBT as 'The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated.'

15. Further information is available in the following IAEA Implementing Guides:

- 'Development, Use and Maintenance of the Design Basis Threat' [11] highlights that the value of the DBT is that it 'provides a detailed and precise technical basis for design and evaluation criteria for physical protection, and can therefore provide greater assurance that the level of protection is sufficient', and it 'also sets a baseline against which the need for changes in physical protection can be evaluated, and provides a clear basis for defining the physical protection responsibilities of the operator'.

- 'Security of Nuclear Information' [12] highlights that the 'The state's relevant competent authorities should develop and issue policy and requirements specific to the security of sensitive information at nuclear material and other radioactive material associated facilities and activities… taking into account the special nature of the activities that involve such materials…the competent authorities should also maintain close liaison with the national security authorities in order for the national threat assessment or design basis threat to be devised'.

5. Advice to Inspectors

16. The DBT is a tool to allow nuclear sites / facilities to identify sabotage targets requiring protection due to potential consequences of a malicious act, and design and test security arrangements. Within the UK, the DBT provides a series of planning assumptions about the composition and capabilities of terrorist groups and other adversaries posing a potential threat to the civil nuclear industry. The DBT is issued by the Department for Business Energy and Industrial Strategy (BEIS) and is distilled from a series of threat assessments from a number of lead government departments and agencies. For those with roles and responsibilities within organisations involved in the development, use and maintenance the DBT, see [11].

17. The planning assumptions apply to all UK civil licensed nuclear sites, premises and transports and (in accordance with the graded approach to

nuclear security) should be used by the relevant 'Responsible Persons' to satisfy the regulatory expectations articulated in the UK civil nuclear industry SyAPs. This includes:

(a) Underpinning VAI assessments which identify sabotage targets (SyDP 6.2);

(b) Physical Protection System (PPS) Design considering elements of the DBT such as the insider threat (SyDP 6.3);

(c) Conducting vulnerability assessments (SyDP 6.4);

(d) Supporting the development of security plans (including consideration of measures to mitigate the effects of 'State-responsibility' threats in the DBT);

(e) Demonstrating and assuring that protective security arrangements achieve the relevant graded security outcome in SyAPs;

(f) Devising site-specific scenarios for the 'Operator-responsibility' threats listed, for use in response and contingency planning.

18. There is the potential to be drawn into a detailed focus on wider components of the FSyPs with which the DBT can apply. Whilst it is reasonable to focus on some areas of the DBT's application more than others for various reasons, including known shortfalls for example, inspectors should remain focussed where possible on the broad application of the DBT. The assessment of a dutyholder's application of the DBT should be aimed at addressing the DBT's application across the breadth of FSyPs and SyDPs in support of KSyPPs, and at best, should inform assessments made in respect of specific SyDPs. Proportionality is key within these assessments, and inspectors should ensure that their expectations for the breadth and depth of analysis undertaken, and evidence provided by the dutyholder in respect of the DBT are tempered by the associated categorisation for theft and sabotage; and, in the case of cyber security, the quantity and security classification of any SNI. Another key factor in the determination of proportionality for cyber security is the attack surface. A dutyholder without a network handling SNI, or utilising operational technology that is 'dumb', analogue or electromechanical will gain little from developing a rich TI capability and inspectors should not expect them to do so.

19. During the preparation and planning phases of the assessment, it is important to understand both where and how the DBT is applied, as this can vary depending upon the site / facility. Consulting with site inspectors is essential not just for logistical reasons, but to inform the focus of the assessment by identifying relevant site-specific circumstances. Pertinent regulatory issues can also be identified to facilitate a targeted and proportionate approach.

20. Given that the DBT touches upon a number of specialist areas, it is good practice to engage with relevant specialist inspectors across ONR's inspectorate. For example, the DBT can be used to inform or generate

scenarios for security exercising. Consulting with the Emergency Preparedness & Response (EP&R) inspector provides important historical context to enhance the overall assessment. For the same reasons, it is necessary to speak to the ONR Sabotage, Target Analysis & Review (STAR) team before making an assessment of the DBT's utility in VAI studies. Overall, wider ONR consultation allows for corroboration and internal challenge resulting in high confidence assessments.

21. When assessing the various areas with which the DBT applies, it is good practice to consider the full hierarchy of implementation. By gaining an understanding of the DBT's assimilation within corporate strategy, policy and divisional process guides, the inspector is able to make an assessment as to whether the DBT's application is integrated and sustainable. Following the golden thread through to the working level application provides ONR with a degree of regulatory confidence in the dutyholder's arrangements. Highlighting any disconnect along the management chain would further enable the inspector to isolate areas for regulatory attention and inform future intervention strategies.

22. When assessing the DBT's application, it is important to assess not just that threat scenarios have been used in the design, evaluation and testing of PPS, but that the full diversity of scenarios have been considered. Emphasis is to be given to the consideration of the 'insider' threat in respect of the advantages this kind of adversary has over external adversaries. See IAEA guidance on 'Preventative and Protective Measures against Insider Threats' [13] for further information and IAEA's definition of the term, 'insider'.

23. The DBT is protectively marked at SECRET. This is worth considering when planning the logistics of either onsite or remote assessment activity. The inspector will need to ensure a secure room has been set aside for the assessment of any SECRET documentation linked to or associated with the DBT. Furthermore, it is worthwhile to remind the dutyholder to exercise caution when sending documentation electronically in advance of or in support of the assessment. Certain sites, for various reasons, may not have the arrangements in place to securely hold SECRET information. In this case, the inspector should couch their expectations and adapt their assessment strategy accordingly. See ONR's Security Assessment Principles for the Civil Nuclear Industry (O-S Annexes) Annex F: Categorisation for Sensitive Nuclear Information [2], ONR's 'Classification Policy for the Civil Nuclear Industry' [4] and the HMG Government Security Classifications document.

24. Irrespective of any local restrictions with regard to storing SECRET documents, inspectors should expect mechanisms to be in place, whereby the DBT can be accessed when required. For example, the document may be held corporately off-site, or local arrangements may even be made with neighbouring sites which have suitable storage mechanisms for sensitive material. The latter would require a Memorandum of Understanding (MOU) to be in place.

25. The approach taken to cyber, and information risk management can be considered to be one of a suite of risk management activities by dutyholders when assessing risks at a facility. This guidance provides specific information that is applicable to CS&IA risks to assist dutyholders demonstrate that adequate arrangements are implemented. It is important to recognise that these arrangements may need to be different from those used to manage nuclear safety risks, although there is likely to be benefit in selecting measures that enhance both cyber security and nuclear safety resilience.

26. Information in all its forms and the systems that operate with it, are a critical element in civil nuclear operations. These operations attract risk, and it is essential therefore that dutyholders know what information and associated assets they are responsible for, where they are, and to have mechanisms in place so that they can make informed, practical and business-enabling risk management decisions.

27. Effective Cyber and Information Risk Management encompass a number of relevant aspects detailed in CNS-TAST-GD-7.1 [14]. The risk assessment element should be informed by a current threat assessment. In-house threat assessments are generally considered to be of the greatest value since they are tailored to the specifics of the business. However, these can be informed by threat intelligence from sources such as: the UK DBT, NCSC (which includes CERT UK and the Cyber information Sharing Partnership), the Centre for the Protection of the National Infrastructure and the National Technical Authorities'.

28. In Preparation for and Response to Cyber Security Events (see CNS-TAST-GD-7.5 [15]), incident response plans should be 'informed by threat assessment information from organisations such as the National Cyber Security Centre (NCSC)'.

6. Regulatory Expectation

29. The regulatory expectation placed upon the dutyholder is that their security plan details how the full breadth of threat scenarios laid out within the DBT are applied across a variety of security-related practices, to ensure that PPS and the security regime is designed, evaluated and tested against threats which the dutyholder is expected to protect against.

30. The DBT is key to a number of FSyPs as detailed above. However, the assessment of the DBT's application and the dutyholder's analysis of threat must be assessed across the breadth of the FSyPs and SyDPs covered in any plan submitted for ONR approval. The assessment of a dutyholder's DBT application or analysis of threat within one FSyP is not sufficient to indicate general compliance. The DBT and any relevant threat analysis have a number of applications and should be applied broadly against KSyPP 2 whereby protection systems should be designed, evaluated and tested.
An intervention against KSyPP 2 can represent a standalone assessment or

can support a range of specific assessments against a dutyholder's security arrangements.

31. Beyond the application of the DBT the regulatory expectation placed upon the dutyholder is that their security plan will also detail how they collect and analyse threat intelligence and other threat information from a wide range of sources and agencies, to identify potential adversaries and their attributes and characteristics, as well as the likelihood of possible adversary actions. The analysis should consider whether specific adversary capabilities are relevant to potential targets and enable the dutyholder to respond effectively to relevant emergent threats which may not be captured in a timely manner within periodic reports or represented in the DBT.

Key Security Plan Principles	The Threat	KSyPP 2
Protection systems should be designed, evaluated and tested using the state's Design Basis Threat, which is supported by threat intelligence that provides situational awareness in order to facilitate dynamic response to new and emerging threats and inform security strategy.		

7. Design Basis Threat

32. It is essential that a DBT is used as the basis for the design, evaluation and testing of protection systems to seek assurance that it will meet a defined security outcome. It should be used in conjunction with the assessment principles within this document to ensure that protection systems are designed to provide an appropriate level of defence in line with the graded approach against attempts to:

(a) Steal NM or ORM in use, storage, or transit in order to construct;

i. An Improvised Nuclear Device (IND). The possibility exists that the theft, including repeated theft of small quantities of plutonium, high enriched uranium or uranium-233, could lead to the construction of an IND by a technically competent, well-resourced terrorist group. INDs incorporate nuclear materials designed to result in the formation of a nuclear yield reaction;

ii. A radiation exposure device, which incorporates radioactive and/or NM and is designed to intentionally expose members of the public to radiation; or

iii. A radiological dispersal device, which is designed to spread radioactive and/or NM using conventional explosives or other means (e.g., incendiary).

(b) Carry out an act of sabotage against a site holding NM or ORM, or against a transportation of NM or ORM, in such a manner as to create a radiological consequence.

(c) Compromise SNI and / or technology (including equipment or software utilised on nuclear premises in connection with activities involving NM/ORM in order to facilitate or commit acts of theft or sabotage.

33. When considering the DBT, dutyholders must give due attention to one of the most serious threats facing the civil nuclear industry, which is 'insiders'. The IAEA define the term 'insider' as 'one or more individuals with the authorised access to nuclear facilities or NM in transport who could attempt unauthorised removal or sabotage, or who could aid an external adversary to do so'. The threat from an insider poses a unique problem due to the advantages they have over an adversary that does not have authorised access.

Inspectors should consider

- Has the full range of threats in the DBT been used to:
  - Complete a vital area study for NM/ORM and associated facilities?
  - Underpin the design of their protective security system?
  - Evaluate the efficacy of the protective security system in achieving the appropriate SyAPs security outcome?
  - Develop scenarios to inform security contingency plans?
- Does the security plan apply the DBT across a suitable range of FSyPs?
- Is appropriate consideration given to the threat posed by insiders?

8. Threat Intelligence

34. There is growing regulatory emphasis on threat reporting. Government regulations are increasingly emphasizing the requirement for organisations to use threat reporting to support risk management. The DBT for the civil nuclear industry is reviewed annually and routinely revised every three years. The IAEA recognises that new or emerging threats may require immediate consideration and actions before DBTs can be revised. Therefore, dutyholders should meet the challenges of a changing physical and cyber threat landscape by supplementing the DBT by developing, managing and maintaining a TI capability in order to dynamically identify and respond to the intent and capability of adversaries.

35. Beyond the application of the DBT, it is good practice for the dutyholder to obtain and analyse additional TI through available sources, coordinated through a centralised function, and integrated within internal and external engagement strategies, to enable them to consider and adapt to locally relevant and emergent threats which may not be captured in a timely manner within periodic reports or represented in the DBT.

36. As part of emergency preparedness planning, as outlined in [16], dutyholders are expected to develop 'incremental and escalatory protective security measures that can be quickly implemented in response to increases in threat', and whilst this is largely directed at formal changes to threat and response level, dutyholders 'may exceptionally implement an increased response level in response to credible threat advice received directly from an authoritative and verified local or national source, or where the circumstances at the site warrant it'. It also stresses that a Security Contingency Plan (SCP) 'should reflect other relevant current generic terrorist or domestic extremist threats to mainland Great Britain, and that such threats, even if deemed outside the DBT, should not be ruled out'.

37. TI is important to both physical and cyber fields as threats are often inherently linked; however, it is the cyber threat picture that presents a particularly dynamic and challenging operating environment. Adversarial intent, capability and opportunities are all increasing and evolving at an accelerating rate as the arms race between cyber network defence and cyber network attack intensifies.

38. Cyber-TI provision to inform the sector's understanding of strategic threats and adversary capabilities is an important consideration in the developing 'NBEST' solution for the civil nuclear industry designed to foster intelligence-led advanced penetration test model and keep the UK Civil Nuclear Sector (UK CNS) ahead of rapidly evolving threats to, and vulnerabilities in, software and equipment.

39. Cyber threat reporting was the focus of a work package within ONRs CS&IA's strategic improvements programme designed to develop good working practices in all aspects of the planning, management, delivery and timely use of cyber-TI (often referred to as CTI). Dutyholders, through the ONR driven Chief Information Security Officers (CISO) Working Group (WG) forum engaged in this initiative and were the recipients of three cyber threat products (see references [17], [18] and [19]). This TAG outlines good practice in the generation and use of TI and to provide consistency in the cyber specific elements this leans heavily on those products.

40. Additionally, personnel security concerns can also be mitigated through effective TI management. The Centre for the Protection of National Infrastructure (CPNI) advocate the use of risk management to provide a systematic basis for proportionate and efficient personnel security measures to prevent or deter a wide variety of insider attacks and describes the lack of this capability as a potential indicator of a high vulnerability. Much of the value

of the risk management process comes from the systematic exploration of TI derived from a range of sources that cover the full array of insider activity which dutyholders may face, which could include, but is not limited to sabotage, theft of intellectual property, unauthorised disclosure of sensitive information, and the facilitation of access by third parties [20].

8.1. Aim

41. Dutyholders should use these different types of threat reporting on an on-going basis, within a demonstrable framework that supports an enduring security program. Good practice TI processes should be:

    (a) Governed by a documented planning and review cycle which is proactively developed by dutyholders to service their specific business requirements.

    (b) Supported by identification of dutyholders' assets (including Information Technology (IT) and Operational Technology (OT)), vulnerabilities and ongoing assessment and monitoring of adversary intent and capability towards the organisation.

    (c) Informed by intelligence collection from a range of internal and external sources, with assessments authored by analytical teams with a multi-disciplinary skillset.

    (d) Actionable, timely and designed to service the requirements of different audiences from board to engineer to back-office employee.

42. TI reporting should enable more effective communication and security decision-making for stakeholders at all levels and across organisations' IT and OT operations. It is not possible to do so if organisations simply consume tactical information, such as Indicator of Compromise (IOC) feeds, or solely collect and / or disseminate intelligence from government sources.

43. The use of TI is a dynamic on-going process that needs to be effectively designed and managed. Dutyholders should weigh the relative importance of TI requirements in light of their current priorities, capabilities, budget and security plans. This TAG is not designed to provide guidance on the specifics of asset or vulnerability management as whilst his is inextricably linked to effective TI, this is addressed by FSyPs 6 and 7 and the associated TAGs

44. Dutyholders should make themselves aware of the threats facing them and implement a threat reporting strategy to protect them. However planning, generating, consuming, analysing, disseminating, and responding to TI reporting can be expensive. Dutyholders of different sizes, budgets and staffing levels will have varying capabilities to undertake the good practice identified in this guidance. Smaller organisations will benefit from a smaller and less complicated network to protect and whilst they should not be exempt from implementing good practice wherever appropriate, proportionate

application is fundamental and should be informed by the SyAPs outcomes that need to be achieved. Externally sourced reporting may be accessed in order to reduce the impact of any internal resource constraints.

8.2. Integrating Cyber, Physical and Personnel Threat Reporting

45. Key management from cyber, physical and personnel security functions should be briefed on the overlap between cyber and physical threat vectors and the ways in which blended threats can manifest. For instance, an insider may facilitate a cyber-attack which compromises a Security Management System (SMS) in order to assist a physical attack on the site. This will enable identification of areas in which they can assist and raise awareness. This may result in adoption of new training and processes for physical and personnel security functions. Such changes and practices should be documented and maintained and new staff from both security disciplines should be inducted into this integrated approach.

46. Whilst the TI element of this TAG is focused predominantly on the management of cyber-TI, the principles and structures covered are equally applicable to physical security as part of the existing security risk management regime, and fusion of the two disciplines' TI capabilities are vital to foster a holistic threat picture.

47. In this context it is noteworthy that the recently released Verizon 2020 Data Breach Investigations Report [21] recorded those physical actions were present in 4% of the near 3,950 breaches in a wide variety of sectors investigated, and the trend is that this remains a relatively constant level of activity. Additionally, understanding the security threats posed by Unmanned Aerial Systems (UAS) and how they are likely to evolve have become key issues across all sectors and are addressed primarily in the protective security function; however, mitigations need to consider the evolving cyber security threats around the use of drones which could increasingly become a major network security threat available to a wide range of threat actors used as an initial network infection vector to, for instance, conduct man-in-the-middle attacks, exploit wi-fi protocols, or spoof and jam other signals [22].

9. Defining Threat Intelligence

48. Broadly, TI can be defined as threat information that is contextualised, analysed, assessed and disseminated to help organisations understand those threat actors and associated threat vectors / tactics, techniques and procedures (TTPs) they face, and enable them to respond to, combat or mitigate the risks to the organisation.

49. Threat information is historic information about cyber adversaries that organisations should use to help them guard against recently employed adversary TTPs. However, if an organisation is a high enough priority,

advanced adversaries (States) may use new TTPs against it, and in this case, an approach that relies on historic threat information to protect the organisation will necessarily fail. Dutyholders should, therefore, use not only historic threat information but also TI to drive threat assessments where appropriate.

50. Threat assessment is a structured process exploiting TI and other information to provide a forward-looking predictive assessment of the capability and intent of relevant adversaries against an organisation.
Unlike threat information and TI, which often deal with tactical and current issues, threat assessment helps organisations to understand the future threat environment in order to help manage risk and protect assets in the longer-term.

51. Developing an efficient TI capability to provide effective TI reporting can provide actionable advice that is relevant and appropriate to the specific organisation and will help dutyholders of all sizes to:

(a) Improve situational understanding of direct threats to the organisation and enterprise and emerging threats aligned to the organisation's changing threat surface.

(b) Improve situational understanding of indirect threats to inter-dependencies, interconnected services and sectors, outsourcing, offshoring and neighbouring sites.

(c) Develop a common and dependable understanding of the threat across the UK CNS, providing greater granularity of the threat to specific components of the sector and its emerging technology.

(d) Improve Indicators & Warnings (I&W) and horizon scanning.

(e) Develop a holistic threat landscape for physical and cyber related threats.

(f) Enable prioritised risk-based protection to plan and budget more efficiently.

(g) Prevent cyber incidents through effective threat monitoring and threat hunting.

(h) Prioritise technical security controls.

(i) Detect and respond to cyber incidents more effectively.

10. Levels of Threat Intelligence

52. TI supports users at the Strategic, Operational and Tactical levels. Each level differs in the nature and format of the material conveyed, its intended

audience and its application. There is broadly a clear understanding across the industry of what constitutes strategic intelligence; however, the definition of operational / tactical intelligence levels often lacks clarity, and this does have the potential for people to be talking at cross purposes as the hierarchical structure of the two levels are often interchanged.

53. From the cyber perspective iSight have summarised these in Table 1 [23].

Table 1: Levels of Threat Intelligence

Strategic users	High-level information is used by strategic users, including executive boards, CISOs, CIOs and CTOs and IT managers that enable them to understand trends and make better decisions about security budgets, process improvements, new technologies, and staffing levels. Strategic intelligence helps to minimize risks and protect new business and technology initiatives. • New adversaries emerging to target enterprises in their industry. • New tactics and techniques exploiting weaknesses in current security defences. • New 'attack surfaces' such as mobile devices, data hosted in the cloud, and employee information posted on social networks.
Operational users	Operational users of intelligence, such as IR teams, forensic analysts, and fraud detection departments, need detailed context around alerts and events. They also need in-depth intelligence on attacks and adversaries so they can: • Quickly establish if alerts or events are part of complex attacks. • Expand their investigations to identify other elements in the attacks. • Identify the sources of attacks (a process called 'attribution'). • Determine which systems have been compromised and which systems need to be remediated. The types of intelligence they need for these activities include analyses of malware, breakdowns of targeted attacks, and reports on adversary TTPs.
Tactical users	Network Operations Center (NOC) staff members need valid malware signatures and URL reputations to allow firewalls, malware gateways, IDS / IPS systems, and other gateway security products to stop attacks without blocking legitimate traffic or generating false positives. Infrastructure groups that manage servers and endpoint devices want intelligence about which vulnerabilities are most critical for the enterprise so they can decide which security patches to apply first, and which systems should have priority for patches and configuration updates.

	SOC analysts monitor alerts and decide which ones should be escalated for further analysis. They want relevant, accurate, and timely data fed to their SIEMs, as well as basic context for alerts so they can quickly decide which ones are isolated events and which might be part of complex attacks.

54. MWR offer a different structure incorporating a Technical Threat Intelligence sub-type, which often has a short life span and is defined as 'information, (or more often data) that is normally consumed through technical means...and comprises technical details of an attackers assets, such as tools, command and control channel, and infrastructure' [24]. Whist it is described as differing from tactical TI because it focuses on specific indicators and rapid distribution and response, and therefore has a shorter usable lifespan; this level is often consumed within the tactical / operational level in other structures.

55. The Joint Emergency Services Interoperability Principles (JESIP) doctrine [25] sets the three tiers of command as presented in Figure 1.

Figure 1: Sub-types of Threat Intelligence

56. Different organisations and agencies have different definitions of strategic, operational and tactical levels, and inspectors should expect variations in terminology, particularly at the tactical level. From an ONR perspective defining this is less important than ensuring the right users receive the requisite product to enable them to operate and meet the business requirements. A demonstration of some types of reporting available and the appropriate audience that should receive it is provided in in Appendix 1.

11. A Good Practice Operating Model – The Intelligence Cycle

57. Intelligence is defined as the product resulting from the processing of information and consists of four core functions which can be achieved through the application of the Intelligence Cycle. There are variations on the Intelligence Cycle structure, as described by the Ministry of Defence [26], and as described in this TAG; but whichever model forms the basis of a TI function it should be an iterative process which encompasses the key Direction, Collection, Processing, and Dissemination (DCPD) phases shown in Figure 2.

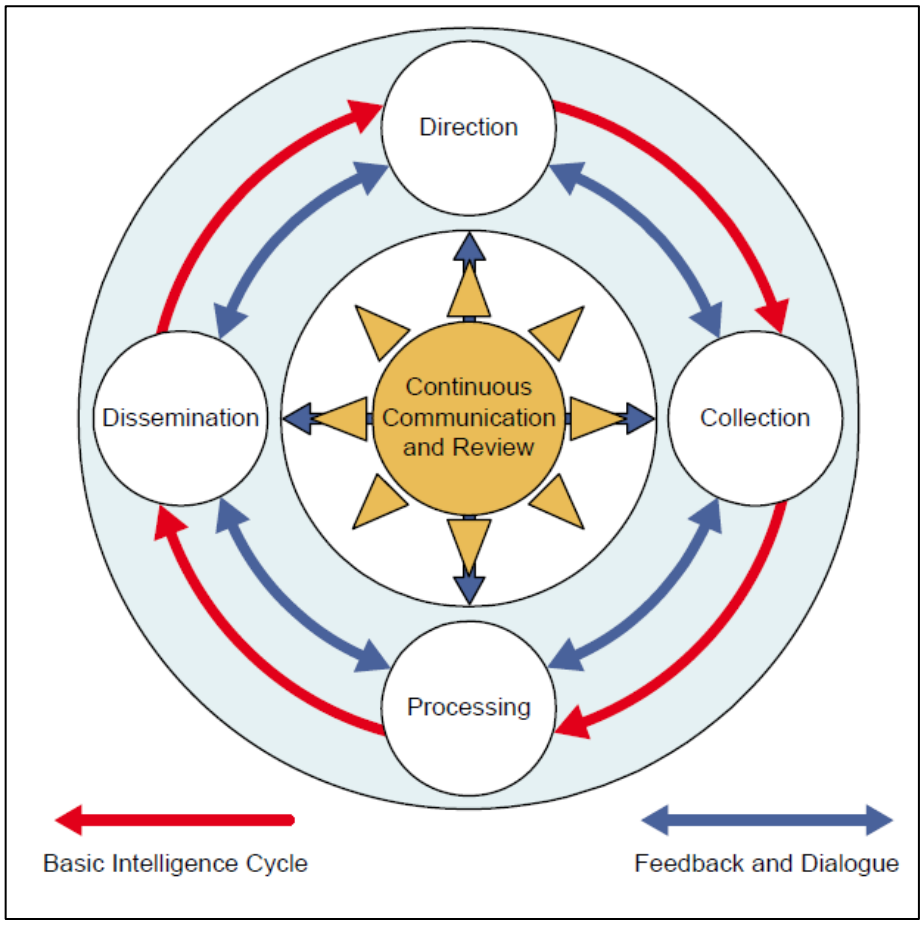

Figure 2: Defence Intelligence Cycle (DCPD)

- **Direction** - The determination of prioritised intelligence requirements and the coordination of a systematic collection effort designed to identify and exploit information sources and intelligence sharing agencies.
- **Collection** - The delivery of all-source information from internal and external providers to the appropriate processing capability for use in the production of intelligence.

- **Processing -** The conversion of information into intelligence through a structured series of actions; evaluation, collation, analysis, integration, interpretation / assessment.

- **Dissemination** - The timely conveyance of accurate and contextualised fused all-source predictive intelligence in an appropriate form, by any suitable means, to those who need it.

58. It is through this process that relevant raw information is collected and processed into actionable intelligence for the benefit of the organisation. Ostensibly a cyclic process, optimal use of the intelligence process is continuous evaluation, feedback, unity of effort (based around information requirements) and the ability to adapt and change focus quickly. The DPCD model is expanded upon at Appendices 1 and 2. The principles of intelligence, which form the bedrock of the intelligence process, are described in Appendix 3.

59. Law enforcement bodies will refer to the National Intelligence Model (NIM) [27] and it has become commonplace to amend the DCPD stages of the Defence Intelligence Cycle into further stages by breaking down those that already exist into their constituent parts, particularly around the processing stage. MWR presented a modified functional TI flow that can be used for a mature scalable TI programme [24]. Whilst similar to the DCPD model, it has some subtle variances and differentiates between intelligence management and execution which is described as useful when building and managing an organisation's teams.

Inspectors should consider

- Has the dutyholder justified selection of an intelligence model, methodology or approach?

- Does the methodology selected represent adequate arrangements to ensure a structured approach to the management of TI?

- Are TI management procedures captured in formalised SPA?

- Is there sufficient maturity (formalised and efficient processes) at each stage of the Intelligence Cycle to collectively deliver a proactive (able to identify intelligence gaps, anticipate future needs and deliver effective assessment) organizational intelligence capability?

12. Vulnerability Assessment and Threat Intelligence

60. Organisations should have a vulnerability management process to assess and prioritise vulnerabilities, including the creation and management of an asset database. At a most basic level this should involve assessment, triage and prioritisation. Assessment should include a clear description of the vulnerability, how it can be exploited, the impact exploitation would have and the mitigations available to reduce associated risk.

61. SyAPs, through SyDP 6.4, expects that 'dutyholders should validate the efficacy of their PPS through the conduct of structured and systematic vulnerability assessments' using a number of proven methodologies; however, these are based on foreseeable threats as defined in the DBT and analysis of the Insider threat. The expectation in KSyPP 2 is that dutyholders will consider threats determined through TI, which may sit outside of the DBT, to identify potential weaknesses to their PPS and seek improvements.

62. For cyber-TI, commonly used collection sources for vulnerability information include common vulnerabilities and exposures (CVE) databases and feeds, as well as industry bodies and vendor and manufacturer websites. Alerting should be as close to real time as possible, and this is available from vendors. The associated patch management policy should focus on patching computers with 'extreme risk' vulnerabilities after which it should be prioritised by an intelligence-informed understanding of which assets are priority targets for adversaries or are being actively targeted.

63. MWR note that some organisations include vulnerability assessment within the scope of the TI function [24]. A close alignment of these to decide whether TI applies to organisational vulnerabilities and being able to act on it is logical. However, there is a subtle distinction. The fact that a vulnerability exists in a product used by the organisation is important information, and requires action, but it's not information about a particular threat. However, information that a particular attack group is exploiting a known vulnerability is TI.

64. Vulnerability assessment should be an on-going, business-as-usual function to detect known vulnerabilities that could have arisen through missed patching or misconfiguration. TI should be responsive to evolving requirements – with clear tasking. Interaction between TI and vulnerability assessment is an element of an effective cyber security risk management process and the relationship between the CPS and vulnerability assessment is considered in more depth in SyDP 7.1.

Inspectors should consider

- Is the PPS vulnerability assessment reviewed in relation to the evolving threat landscape?

- Does the dutyholder have a process in place to prioritise the application of patches across the organisation based on an understanding of adversarial intent and capability?

References

[1] H.M. Government, “The Nuclear Industries Security Regulations 2003 (NISR) (2003/403),” 2003.

[2] ONR, “Security Assessment Principles (SyAPs) for the Civil Nuclear Industry,” 2017.

[3] H.M. Government, “Government Functional Standard GovS 007: Security,” [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903904/Government_Security_Standard.pdf.

[4] ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civl Nuclear Industry”.

[5] NCSC , “NCSC Cyber Assessment Framework, A.2 Risk Management,” [Online]. Available: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a2-risk-management.

[6] IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM)”.

[7] IAEA, “Nuclear Security Series No. 20. Objective and Essential Elements of a State’s Nuclear Security Regime”.

[8] IAEA, “Nuclear Security Series No 14. Nuclear Security Recommendations on Radioactive Material and Associated Facilities”.

[9] IAEA, “Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),” 2011.

[10] IAEA, “Design Basis Threat,” [Online]. Available: https://www.iaea.org/topics/security-of-nuclear-and-other-radioactive-material/design-basis-threat.

[11] IAEA, “Nuclear Security Series No. 10. IAEA Implementing Guide: Development, Use and Maintenance of the Design Basis Threat”.

[12] IAEA, “Nuclear Security Series No. 23-G IAEA Implementing Guide: Security of Nuclear Information”.

[13] IAEA, “Nuclear Security Series No. 8-G - Preventive and Protective Measures against Insider Threats”.

[14] ONR, “CNS-TAST-GD-7.1 - Effective Cyber and Information Risk Management (2019/135696)”.

[15] ONR, “CNS-TAST-GD-7.5 - Preparation for and Response to Cyber Security Events”.

[16] ONR, “CNS-TAST-GD-10.1 - CT Measures, Emergency Preparedness and Response Planning”.

[17] ContextIS, “UK Civil Nuclear Sector Cyber Threat Assessment,,” 2018.

[18] ContextIS, “Cyber Threat Reporting Good Practice Guide,” 2018.

[19] ContextIS, “Cyber Threat Reporting Good Practice Guide for Senior Management,” 2018.

[20] CPNI, “Insider Risk Assessment,” [Online]. Available: https://www.cpni.gov.uk/insider-risk-assessment.

[21] Verison, “Verizon 2020 Data Breach Investigations Report,” [Online]. Available: https://enterprise.verizon.com/en-gb/resources/reports/dbir/.

[22] H. A. Booz, “Top 9 Cybersecurity Trends for 2020,” [Online]. Available: https://www.boozallen.com/c/insight/publication/top-9-cybersecurity-trends-for-2020.html.

[23] M. B. Jon Friedman, Definitive Guide to Cyber Threat Intelligence, CyberEdge Press.

[24] MWR InfoSecurity Ltd, “Threat Intelligence: Collecting, Analysing, Evaluating”.

[25] JESIP, “Tiers of Command,” [Online]. Available: https://jesip.org.uk/command.

[26] Ministry of Defence, “Joint Doctrine Publication 2-00 - Understanding and Intelligence Support to Joint Operations (3rd Edition),” 2011. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

[27] Home Office, “National Intelligence Model Code of Practice,” [Online]. Available: https://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf.

[28] CREST, “What is Cyber Threat Intelligence and how is it used?,” 2019. [Online]. Available: https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf.

[29] US Joint Cheifs of Staff, “Joint Intelligence,” 2007. [Online]. Available: https://www.jcs.mil/portals/36/documents/doctrine/pubs/jp2_0.pdf.

[30] The National Cyber Security Centre, “The Cyber Security Body of Knowledge,” 2019. [Online]. Available: https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf.

[31] The National Cyber Security Centre, “Introduction to logging for security purposes,” 2018. [Online]. Available: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.

[32] The National Cyber Security Centre, “Device Security Guidance,” [Online]. Available: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring.

[33] CyberEdge, The Threat Intelligence Handbook, Pace.

[34] Lockhead Martin, “Gaining the Advantage - Applying Cyber Kill Chain Methodology to Network Defence,” [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

[35] The MITRE Corporation, “MITRE ATT&CK,” [Online]. Available: https://attack.mitre.org/.

[36] The MITRE Corporation, “D3FEND™ - A knowledge graph of cybersecurity countermeasures,” [Online]. Available: https://d3fend.mitre.org/.

[37] Verisign Public, “White Paper - Establishing a formal cyber security intelligence capability,” [Online].

Glossary and Abbreviations

BEIS	Department for Business, Energy and Industrial Strategy
CISO	Chief Information Security Officer
CPNI	Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
CPS	Cyber Protection System
CS&IA	Cyber Security & Information Assurance
CVE	Common Vulnerabilities and Exposures
DBT	Design Basis Threat
DCPD	Direction Collection Processing Dissemination
EP&R	Emergency Preparedness & Response
FSyP	Fundamental Security Principle
I&W	Indicators and Warnings
IAEA	International Atomic Energy Agency
ICP	Intelligence Collection Plan
IND	Improvised Nuclear Device
IOC	Indicator of Compromise
IR (CIR / PIR / SIR)	Intelligence Requirement (Critical / Priority / Specific)
IT	Information Technology
JESIP	Joint Emergency Services Interoperability Principles
KSyPP	Key Security Plan Principle
MOU	Memorandum of Understanding
NCSC	National Cyber Security Centre
NIM	National Intelligence Model
NISR	Nuclear Industries Security Regulations 2003
NM	Nuclear Material
NSS	(IAEA) Nuclear Security Series
NSSP	Nuclear Site Security Plan
NTA	National Technical Authority
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
OT	Operational Technology
PPS	Physical Protection System
RFI	Request for Information

SCP	Security Contingency Plan
SIEM	Security Information and Event Management
SMS	Security Management System
SNI	Sensitive Nuclear Information
SOC	Security Operations Centre
SPA	Standards, Procedures & Arrangements
STAR	Sabotage, Target Analysis & Review
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide
TI	Threat Intelligence
TSP	Transport Security Plan
TSS	Transport Security Statement
TTP	Tactics, Techniques and Procedures
UAS	Unmanned Aerial Systems
VAI	Vital Area Identification
WG	Working Group

Appendix 1: The Intelligence Cycle – Direction and Collection

Direction

1. Direction refers to the leadership decision of collection and analysis priorities to meet business requirements. Decision makers need to identify what they specifically want to know and what the TI programme should be telling them. Ownership and control of the intelligence capability ensures responsiveness and accountability are embedded as central operating features. Overall strategic direction sets the requirements and priorities through what are sometimes referred to as Critical Information Requirements (CIR) which provide a broad thematic platform from which Priority Intelligence Requirements (PIR) (or Key Threats) are used to determine and prioritise all forms of collection for the key threats facing the organisation.

2. In this way, analytical resources are tasked against documented PIRs which are typically agreed by the board and security managers within the organisation. PIRs are often broken down into subsets such as Specific IRs (SIR) to add granularity to the overarching and often high level PIRs. This is done to ensure collection assets are effectively tasked and all elements of information are answered.

3. There are many areas where a dutyholder's security decision-making will benefit from effective use of threat reporting in order to meet business requirements. Circumstances include:

   (a) The organisation is undertaking a thorough risk assessment and needs threat reporting to inform both the range of risks and the likelihood of them occurring.

   (b) The board has limited understanding of the cyber threat landscape and requires evidence-based and customised reporting.

   (c) The organisation is considering outsourcing IT services to a Managed Service Provider (MSP) or cloud service provider and needs to know how that move will change their threat surface.

   (d) The organisation is undertaking a process of TI informed assurance activity and requires identification and assessment of adversary intent and capability in order to design realistic scenarios for a red team.

   (e) The organisation requires current intelligence on a priority adversary in order to conduct targeted threat detection and historic threat hunting activities or to prepare and test Incident Response plans.

(f) The organisation wants to implement the most effective technical mitigation measures and needs to choose them in an evidence-based manner.

(g) The organisation has inter-dependencies and inter-connectivity with external services and sectors that could constitute an indirect threat.

4. Decision makers should identify what they specifically want to know and what the threat programme should be telling them. Adversarial intent and capability in relation to the organisation's critical assets should be key. The full range of threat actors, their TTPs and trends and developments in threat vectors should be considered in order to prioritise implementation of appropriate business and technical controls to protect important assets and prevent future attacks paths.

5. CIRs are used to develop an intelligence collection plan (ICP) to coordinate and prioritise collection activities. Tactical and operational direction can be an internal tasking of the cyber threat capability, but strategic and some operational requirements will be directed to external sources and agencies. These are often represented in a formal ICP designed to identify and exploit available sources. ICPs are typically presented as a spreadsheet with PIRs / SIRs along the vertical axis and available sources to be tasked along the horizontal axis. An example basic ICP is provided at Figure 3.

						Internal				External				
Ser	CIR	PIR	SIR	Priority	Report Recipient	SOC	IT	ICS	IR	NCSC	BEIS	CPNI	Ind-100	CTSA
1	What are the indirect threats to the business?	What is the threat to our sector dependencies?	0101. What is the threat to the Energy Sector?	1	Execs, CISO					x	x	x	x	x
			0102. What is the threat to the Transport Sector?	1	Execs, CISO					x	x	x	x	x
2	What is the cyber-crime threat to CNS?	When, and with what frequency, are we subjected to cyber attacks?	0201. What % of emails rejected as malicious contained malware or phishing links?	2	CISO, IT Manager	x	x		x					
			0201. What is the monthly average of DOS attacks on the network and application layers?	2	CISO, IT Manager	x	x		x					
		What threat actors target the CNS and what vectors are used?	0203. Who are the groups/ individuals involved in energy sector ransomware attacks and what TTPs have they used?	1	Execs, CISO					x	x		x	

Figure 3: Example ICP extract

6. An effective ICP requires oversight, close management and continuous review to ensure that intelligence collection efforts remain relevant to the business needs and analytical resources are tasked against documented IRs. Engagement and close liaison with available sources of information is key to

identifying the viability in meeting IRs and this interaction should be underpinned by a formalised means of processing and recording requests for information. This may necessitate comprehensive interconnectivity with other stakeholders with information exchange using appropriately accredited networks.

7. Strategic direction of TI management is critical in aligning delivery to meet business objectives and feed requirements on the key threats to the organisation. The determination of PIRs / SIRs and coordination of a systematic all-source collection effort, would underpin the processing of information and intelligence. This should prevent, for instance, the analysis effort in monitoring networks for malicious or suspicious traffic being reliant on best endeavours of the analyst rather than being derived from a prioritised set of requirements.

8. A Request for Information (RFI) may be driven by the intelligence function or customers, where appropriate, to deliver Tactical or Operational level requests for information or intelligence that supports existing CIRs. These would be considered based upon function, scope and capability, capacity to meet the requirement timeframe, and priority in relation to existing tasks. The RFI would ideally be presented in a standardised format that would define; who is asking for the information; when is it required by; what format it is required in; what is the context to why the RFI is being generated; what the specific ask is; and whether there are any specific handling instructions. This will help enable the effective managing and tracking of RFIs.

Inspectors should consider

- Does the dutyholder have a formalised set of Board driven intelligence requirements that align its TI delivery to meet business objectives?
- Does the dutyholder have a formalised means to track and manage RFIs?
- Does the dutyholder have a systematic all-source collection effort that identifies and exploits available internal and external sources and agencies to deliver data, information and intelligence for processing?
- Does the intelligence plan support threat reporting that educates staff and improves decision-making across the ‘plan-prevent-detect-respond-recover’ lifecycle?
- Does the organisation have a documented intelligence plan which captures and validates the business' intelligence requirements and the means to address them?

Collection

9. Information and data can come from a large variety of sources. Understanding which sources are available, exploitable and likely to produce the desired information reliably and in an actionable and timely manner is critical in meeting the requirements identified in the Direction stage. Dutyholders should therefore employ an all-source collection model involving collection from as many appropriate, relevant sources (both internal and external) as possible.

10. Dutyholders should identify their current intelligence gaps and address them through procurement of appropriate reporting. Table 2 demonstrates some types of reporting available from some of the key sources available; however, this is not exhaustive.

Table 2: Sample sources, products, feeds and forums

Source	Products/Feeds/Forums/Agencies/Organisations
Internal	SOC, IT, NOC, IR, ICS
Government / Law Enforcement	Advice, Briefings, Reports, Digests, Assessments lessons learned from Centre for the Protection of National Infrastructure (CPNI) website / extranet, National Counter Terrorism Security Office (NaCTSO) Counter Terrorism Security Advisors (CTSA), Local Police Constabularies / Special Branch, CNC, British Transport Police, National Crime Agency (NCA) website, Action Fraud, Cabinet Office, NCSC, BEIS Cyber Security Oversight Group (CSOG) Energy Emergency Executive Committee (E3C), Local Authorities.
Industry Sharing	Advice, Briefings, Reports, Digests, Assessments, lessons learned from Cyber Security Information Sharing Partnership (CiSP), Industrial Control System (ICS) – Computer Emergency Response Team (CERT) advice, ICS-ISAC advice, CISO Working Group, NDA Civil Nuclear Threat workshop, NCSC Industry 100, Counter UAS (C-UAS) Working Group, Action Fraud, Malware Information Sharing Platform (MISP), Security Awareness Special Interest Group, SANS webinars and products
Opensource and social media	Media (foreign affairs, technology and security), Alerts, Threat feeds, Intelligence Reports, Annual Reports, Paste-bin, Think Tanks, Academic resources such as CyBOK, security blogs, security professionals' Twitter feeds
Vulnerability	Supplier, Industry databases
Security Products	Anti-Virus, IPS, IDS, Sandboxes
Vendor Reporting	Feeds from Threat Intelligence Platforms, Alerts, Threat feeds, Intelligence Reports, Annual Reports, Paste-bin, APT profiles, free and commissioned reporting industry leading forums such as the Information Security Forum's Threat Horizon initiative

Relationship between Data, Information and Intelligence

11. Intelligence in this context can be defined as the product resulting from the processing of information concerning the activities of individuals and organisations of broad concern to the dutyholder and its ability to function securely. This encompasses the risks posed by nation states, terrorist organisations, organised crime groups or criminals, insiders, single-issue groups, hacktivists, investigative journalists and other disruptive elements. Information differs fundamentally and is defined in [26] as unprocessed data of every description that may be used in the production of intelligence. In some instances, intelligence from other organisations or agencies may be considered as information until it has had a degree of processing to re-evaluate.

12. In the context of cyber-TI, CREST describe the raw material from which intelligence is derived as data and information. They define data as simple facts that tend to be available in large volumes; IP addresses or logs are typical examples. By itself, raw data is of limited utility. Information is produced when this data is collated to provide a useful output – for example, a collated series of logs showing a spike in suspicious activity. Intelligence comes from the processing and analysis of this information and can be used to inform decision making. For example, the collated log data is contextualised with prior incident reports regarding similar activity, which also allows for the development of a strategy to mitigate the incident [28].

13. The relationship between data, information and intelligence is illustrated in US intelligence doctrine [29] and shown in Figure 4. This aligns to the phases of the Intelligence Cycle described above, with each lens offering opportunity to determine I&W to be extracted from available sources.

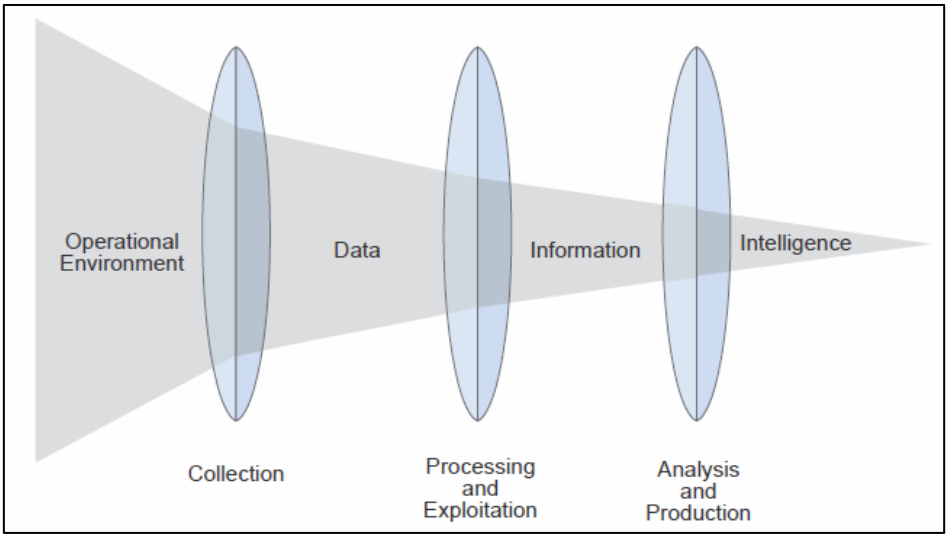

Figure 4: Relationship between data, information and intelligence

Collection – Internal Sources and Required Data Feeds

14. Internal sources of intelligence are an important part of an organisation's overall intelligence picture. Good internal intelligence enables organisations to identify both unsuccessful and successful intrusion attempts, defensive weak spots and critical assets. It also helps in determining and prioritising security measures. Controlled internal sources of information in the physical sphere are likely limited to security force patrol activities, integral surveillance such as CCTV (and potentially UAS), and casual sources of information such as contractor / staff reporting stimulated through an instilled workplace security culture.

15. From a cyber-TI perspective internal teams will use intelligence reporting to select appropriate signatures and IOCs to feed into the organisation's security products. Such products could include next-generation firewalls, endpoint protection software, intrusion detection or prevention systems etc. The types of internal intelligence technical teams typically generate are incident reports, anomalous account behaviour, network activity and device behaviour.

16. Dutyholders should centrally aggregate internal and external gathered intelligence, via the Security Operations Centre (SOC), if applicable. It is important to allow for various data types, which must be indexed and be able to be queried easily. This collected intelligence should feed into internally used security products, which will provide alerts. Those alerts need to be monitored, triaged, investigated and escalated to Incident Response (IR) teams where necessary. IR teams can investigate serious events, respond to intrusions and recommend improvements or additional technical controls to prevent similar future attempts. Reports can then be written on any incidents and a brief for senior audiences provided where necessary.

17. To monitor threats to computer systems, whether the goal is to generate TI or to investigate and contain an on-going incident, it is critical that network defenders and threat analysts have visibility of activity on the network. The dutyholder should collect sufficient logs from key aspects of their networks as a source of intelligence, deploying additional software and hardware capabilities to supplement or enable this as required. Routine log reviews and analysis are beneficial for identifying and resolving security incidents. Logs can also be useful for performing forensic analysis post-breach, supporting the organisation's internal investigations, establishing good baselines, as well as supporting investigations and remediation by external providers. Logs must be stored in a secure manner.

18. Key to this activity, and in successfully generating and consuming intelligence, is knowing not only the intelligence value of data sources (Table 3 provides examples of the types of intelligence that can be derived or applied to common data sources), but more importantly recognising that the value of the data in a correlated form is greater than individual log files. This allows the identification of enterprise-wide threats and provides the ability to respond with increased confidence. In order to act on or derive intelligence it is the linkage

between these logs that provides the most business benefit to generate not only insight, but foresight too.

19. For example, if web analytics indicates that the Distributed Denial of Service (DDoS) service has failed to block traffic from a suspicious Internet Protocol (IP) non-UK address, this will require verification and application logs to be reviewed for source IP addresses and http headers that indicate the true source of the connection. On review, these logs show a Structured Query Language (SQL) injection attack has occurred that causes the back-end database to export records of File Transfer Protocol (FTP) to an obscure domain name. Domain Name System (DNS), Data Loss Prevention (DLP) and database logs are then investigated to verify this. These results may generate an intelligence report and given the nature of the incident would include recommendations on web application filtering and database configuration.

20. On-boarding logs into an analytical environment should be prioritised based upon business requirements. If a high risk to the enterprise is deemed to be from business email compromise (BEC) style phishing scams, then prioritising those log data sources associated with the end-to-end email journey may be appropriate in order to enable detection, analysis, validation and response to counter the delivery, exploitation and communication of malicious emails. However, this may be deemed secondary to log data from a variety of other sources essential to tracking, for instance, insider activity.

Table 3: Data sources and intelligence value

Data Source	Intelligence Value
Anti-Virus	Identify malware has been introduced – answer the question whether it is malicious or accidental.
Application Logs	Specific transaction types, source of attack, type of attack, data extraction occurring.
Database Application Monitoring	Transactions issued against databases; are they authorised? Bulk data downloads, obscure destinations.
Data Loss Prevention	Identify where unauthorised extracts of data are taking place.
DDoS	Identify denial of service attempts, blocked countries, analyse block access.
DNS	Identify potential routes of communication, e.g., botnets attempting to ‘call home’.
Firewalls	Successful and failed attempts to infiltrate networks and/or extract data.
Full Packet Capture	Forensic analysis in the event of an incident.
Identity and Access Management	Link identities to threats derived in the other event log sources.
Integrity checking	Identifying if key files have been changed on critical infrastructure.

Data Source	Intelligence Value
Intrusion Prevention	Identify specific threats attempting to be exploited.
Operating System Logs	Commands issued against critical infrastructure; by who and where from.
Social Media	Indicator of emerging threats and / or immediate threats to the organisation and partners.
Vulnerability Intelligence	Mapping of systems to vulnerability databases –used in the absence of vulnerability scanning.
Vulnerability Scanning	Identifying vulnerable services to enable effective risk assessment.
Web Analytics	Path taken through external systems; end client intelligence.
Web Application Firewalls	Identify specific threats being attempted to be exploited.

21. The Cyber Security Body of Knowledge (CyBOK) project [30] expands on this and offers a conceptual view of possible data sources and describes those data logs associated with either: host behaviours reporting on operating systems or applications; or network behaviours reporting communication patterns that generate information of interest from a security perspective. It also highlights how the move to external resources such as cloud providers or internet service providers may limit the availability of some of the data sources for practical reasons such as volume, or due to privacy constraints and entanglement of multiple customer data in the same trace.

22. Expectations regarding basic good practice for logging if: a dutyholder currently has little or no logging capability; a dutyholder would like to assess the suitability of their current logging capability; or a dutyholder would like to be better prepared for a cyber-incident, is provided by NCSC [31]. Their guidance proposes a four-step program for putting in place a simple but effective logging capability, whilst guidance and advice is also provided on the use of logging and monitoring to identify threats and protect smartphones, tablets, laptops and desktop computers [32].

Collection – External sources

23. While risk management is the dutyholder's responsibility, a dutyholder's assessment of their threat environment should be guided by threat advice provided by external sources. For higher priority targets, such as the nuclear industry, external sources are likely to be more crucial. External sources can help organisations to identify, mitigate and respond to threats of which they were previously unaware.

24. As with internal reporting, external reporting and feeds are only useful if the receiving organisation uses the data provided. This includes use in firewalls,

security and information event management (SIEM) systems, endpoint protection software and network-based security technologies.

25. There is a very broad range of free and paid-for sources offering specific industry and generalised threat reporting at strategic to tactical levels, as provided in Table 3, which dutyholders should exploit to improve threat reporting around cyber, physical and personnel security.

26. Dutyholders should establish, maintain and resource information sharing groups for the nuclear industry and sector interdependencies (such as National Grid, Supply Chain, Transport Sector etc) and interconnectivities (wider business interests, data centres, Cloud services, MSPs) that will facilitate sharing of information within the UK nuclear sector and between the industry and national technical authorities in order to collectively inform the strategic perspective of the physical and cyber threats.

Identifying and Filling Collection Gaps

27. A review of collected information should be conducted to identify if all pre-determined IRs have been met. Any unmet IRs should be documented and a source of information to fill the gap should be identified.

28. Dutyholders can outsource this function to external providers where necessary. Independent validation can be sought to ensure there are no unknown gaps in IRs or security controls. External providers should be judged by their ability to reliably identify any collection gaps the organisation has and to provide clear guidance on how these gaps can be addressed.

Inspectors should consider

- If the dutyholder utilises a commercial vendor for the delivery of its TI, what assurances do they have around the protection of its data (if appropriate), and how do they engage to ensure its collection activities are current or changeable to meet developing requirements to meet business objectives?
- Has the dutyholder established mechanisms with other industry and government stakeholders to engage in information sharing forums to inform the strategic perspective of TI?
- Does the dutyholder have a formalised approach and follow good practice in their log management programme?
- Does the dutyholder have formalised processes for bridging intelligence gaps in their collection coordination and information requirements management?

Appendix 2: The Intelligence Cycle – Processing and Dissemination

Processing

1. Processing is a structured series of actions – evaluation, collation, interpretation, analysis, and interpretation / assessment – which although are set out sequentially for ease of understanding, are likely to take place concurrently, whilst tactical data feeds may require a less integrated approach to generate I&W.

2. Evaluation. This is an appraisal of an item of information in respect of the reliability of the source and credibility, or plausibility, of the information. In addition, there may be potential third-party distortion / inadvertent distortion to the information accumulated during pre-processing. This is a vital component which in effect begins with receipt of information in the Collection stage, since whilst much information may be received from trusted sources such as government agencies and National Technical Authorities (NTA), some will include open-source intelligence as well as dedicated feeds provided by commercial companies.

3. Collation. Related items of information or intelligence are grouped together to provide a record of events to facilitate further processing. In practise this is made up of procedures for receiving, grouping and recording reports. The following factors are often taken into consideration in this phase: standardisation, cross-referencing (including metadata tagging) and prioritisation to ensure incoming information is treated with an appropriate degree of urgency.

4. Analysis. Information is subject to a systematic, logical and reasoned analysis process, drawing on corporate knowledge and understanding supported by analytical tools and techniques to establish meaning and context to identify significant facts for subsequent interpretation. The use of structured, quantitative and qualitative analytical techniques (of which there are hundreds) should be used to challenge judgements, identify mental mind-sets, stimulate creativity and manage uncertainty. They help to counter bias (mental tendencies and prejudice), fallacies (faulty reasoning) and deception. They also reinforce the generation of hypotheses and assumptions. The latter is vital as it helps to strengthen and build confidence in analysis, develops new hypothesis, and is important in the absence of fact.

5. Integration. Integration relates to the fusion of disparate information from a variety of diverse sources (including cyber and physical) into a coherent entity in order to identify patterns and generate a completer and more holistic picture of the environment or situation. In practice integration follows on from analysis without a break and in effect the two processes are often treated as one.

6. Interpretation / Assessment. Interpretation is the final stage of processing in which the significance of information / intelligence is judged in relation to the current body of knowledge. Assessment is the term commonly used to describe this activity and its result. Assessment is both a process and an outcome. The process is defined as an objective mental process of comparison and deduction based on common sense, experience, and knowledge, covering both existing information and intelligence. Within the process, new information or intelligence is compared with, or added to, that which is already known, giving rise to new or updated intelligence. The resulting outcome or product is the assessment. Assessments should be predictive and actionable.

7. Whilst these Processing stages are a central tenet for managing strategic and operational intelligence, tactical intelligence may require a less integrated approach to generate I&W that should subsequently be confirmed by more considered multi-source intelligence analysis. A potential intelligence workflow for internal technical teams is illustrated in Figure 5.

Figure 5: Potential intelligence workflow for internal technical teams

Cyber Threat Intelligence Frameworks

8. CyberEdge [33] commends the benefits of using TI frameworks ‘to promote a broad understanding of how attackers think, the methods they use, and where in attack lifecycle specific events occur’. These may benefit dutyholders as they ‘provide structures for thinking about attacks and adversaries and this knowledge allows defenders to take decisive action faster and stop attackers sooner’ and proactively detect persistent threats. Two are considered further; the Cyber Kill Chain [34], and MITRE ATT&CK® framework [35] and described in Table 4.

Table 4: Overview of sample Threat Intelligence frameworks

Cyber Kill Chain®	MITRE ATT&CK® Framework

Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective. The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures. The defender's goal is to understand the adversary's actions, and that understanding is delivered by TI. The Cyber Kill Chain allows organizations to build a defence-in-depth model that targets specific parts of the kill chain. For example, acquiring 3rd -party TI to monitor: • References to your enterprise on the web that would indicate reconnaissance activities • Information about weaponisation against newly reported vulnerabilities in applications on your network.	MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cyber-security product and service community. ATT&CK is open and available to dutyholders for use at no charge. ATT&CK Matrices cover adversarial tactics and techniques affecting the Enterprise, mobile device access and network-based effects that can be used by adversaries without device access, and ATT&CK for ICS is a knowledge base useful for describing the actions an adversary may take while operating within an ICS network. These can be used to better characterize and describe post-compromise adversary behaviour. ATT&CK builds on the Cyber Kill Chain, but rather than describe a single attack, it focuses on the indicators and tactics associated with specific adversaries. It uses 11 different tactic categories to describe adversary behaviour. The MITRE D3fend framework provides defensive techniques that can be applied to counter the practices detailed in the ATT&CK matrix [36].

Writing for Effect

9. In order to use threat to influence decision-makers, reporting should be:

   (a) Bespoke and Actionable. Threat reporting should directly relate to the organisation, containing explicit assessments and findings that enable actions to be taken.

   (b) Well-formatted. The key information that is intended to influence the reader must be well signposted and be easily and quickly digestible.

(c) Peer-reviewed. Where necessary, the extent to which a report has been peer-reviewed should be made clear.

(d) Presented to a prepared audience. Decision-makers may benefit from prior review of threat reporting ahead of a decision-making group meeting.

(e) Presented at the right time. The delivery of some threat reporting may need to be closely tied to the timing of the decision / requirement it is supporting. Early dissemination may weaken impact; too late, it cannot possibly inform decisions.

Understanding Intelligence Reporting

10. Confidence levels. Doubt in an intelligence assessment is made transparent to customers and annotated in a uniform and consistent manner. Confidence levels are reliant on the analyst's experience, judgement and intuition, and provide a descriptive value to conclusions, but can be expanded in text to convey confidence assessments.

Table 5: Confidence Levels

Level	Summary
HIGH	Good quality of information, multiple evidence from different sources where possible to make a clear judgement.
MODERATE	Evidence open to various interpretations or is credible / plausible but lacks correlation.
LOW	Fragmentary information or sources suspect reliability.

11. Probabilistic language. The use of qualitative expression of probability in assessment is in itself problematic. A standardised measure – the uncertainty yardstick – is used to make assessments consistent and provide some context to the terminology used.

Table 6: Probabilistic Language

Statement	Probability
Remote/Highly unlikely/Almost certainly not	<10%
Improbable/Unlikely/Probably not	15-20%
Realistic probability	30-50%
Probably/likely	60-70%
Highly likely/Very probable	75-85%
Almost certain	>90%

12. The intentional gaps between the ranges are to encourage intelligence analysts to be clear about the meaning of their intelligence assessments. This precludes a debate about whether something is at the lower and of one range or the upper end of the range below it.

Using Threat Assessments to Future-Proof Decision-Making

13. Dutyholders should use threat assessments to:

    (a) Evaluate the effectiveness of their current and planned security posture in light of adversaries' intentions and capabilities.

    (b) Evaluate their ability to monitor, detect, mitigate, prevent and remediate targeted physical / cyber intrusions by the adversaries referred to in the report.

    (c) Future-proof longer-term security decision-making by providing logical and predictive assessment of future threats to the organisations.

14. Assessments of adversaries' capabilities should be compared with, for example, the dutyholder's knowledge of its network vulnerabilities to identify areas for improvement. The intentions of particular adversaries with capabilities that exceed current defences should be used to guide the timeframes for closing the gap that exists between the adversary capability and the organisation's defences.

15. Inspectors should consider:

- Is the analysis effort in monitoring networks for malicious or suspicious traffic driven by a prioritised set of requirements, rather than a reliance on experience, skill, judgement and awareness of the analyst?
- Is the processing of data / information underpinned by prioritised intelligence requirements and coordination of a systematic all-source collection effort designed to deliver effective and predictive TI to support business objectives?
- If the dutyholder utilises a commercial vendor for the delivery of its TI, what assurances do they have around the protection of its data (if appropriate), and how do they engage to ensure its collection activities are current or changeable to meet developing requirements to meet business objectives?
- Does the dutyholder utilise trained specialists to analyse cyber threats, vulnerabilities and potential impacts?

Dissemination

16. Dissemination is the final stage of the Intelligence Cycle and can be defined as the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. This is a key activity, as without efficient and effective dissemination the value of the intelligence processing is largely lost.

17. Direction, or customer requirements, which dissemination feeds, must be sought and clarified, and dissemination capabilities must be considered when processing information. The expectation would be that frequency of dissemination is likely to match the time period on which the content is based with operational material disseminated more frequently than, for instance, strategic content which is likely to be more irregular. User feedback is a vital element of the continuous review process which underpins the Intelligence Cycle to ensure effective products and IR refinement. Feedback can be formalised and defined to help deliver a measure of the impact of threat reporting which could at the lowest level have provided no increased understanding of an issue, to the highest level which could have directly influenced Board level decision, affected policy or provided the requisite information to generate intelligence led risk-based decisions on significant emerging threats to the organisation.

18. There are a number of factors which affect effective dissemination. Reports should demonstrate accuracy, brevity and clarity to ensure there is differentiation made between facts and interpretation of them. Intelligence is time-sensitive and should be dated, including a cut-off date where appropriate, to demonstrate timeliness. The product should meet a current need and be tailored to meet requirements in an appropriate format / medium as requested by the demander. Outputs should also be standardised and compiled in accordance with standing product lines and formats which can take an innumerable number of forms from standalone documents to a constant feed of information or a continuously up-to-date database.

19. These characteristics, especially timeliness and accuracy, can be particularly challenging in the cyber domain where near-real time reporting and automated I&W of network attacks should be a requirement of a cyber-TI capability.

Reporting for Different Stakeholders

20. To satisfy the intelligence needs of stakeholders at different levels, dutyholders need to consider the different types of reporting that can be employed. Some audiences will only receive reporting to inform future decision-making, while others will be expected to act upon reporting immediately. General employees may be given some strategic level reporting to reduce their resistance to technical control implementation and to help prevent circumvention of existing controls and procedures. In all cases the product should be designed and delivered in the right format for the specific audience.

21. Dutyholders should lead on the development of an appropriate mechanism for the sharing of threat reporting amongst organisations with significant foreign ownership or control, and should, where possible, share threat reporting with other organisations in their sector and supply chain.

22. Table 7 demonstrates some types of reporting available and the potential audience that should receive it.

Inspectors should consider

- Is the dutyholder able to demonstrate adequate arrangements for delivering a threat picture that is tailored to the specific Strategic, Tactical and Operational requirements of the business?
- Does the dutyholder's TI function deliver a threat picture that covers the full spectrum of vectors associated with the key threat actors?
- Is the dutyholder able to describe the current procedures that would deliver Strategic TI to the Executive Team, and Operational / Tactical TI to middle management / Technical Teams? Are these TI processes captured and formalised in SPA?
- Does the dutyholder's TI function support the delivery of new projects and other initiatives, and prompt lessons learned to drive continuous improvement and facilitate a more robust and effective TI strategy?
- Is the dutyholder able to demonstrate good practice in accessing and consuming threat reporting to provide education, understanding and threat-informed mitigation strategies in order to counter, for example, the threat from phishing and help instil an effective workplace culture?
- How is TI used to inform incident lessons learned and the organisation Incident Management Strategy?
- Does the SCP address all relevant threats identified within the DBT and additional threats identified in the TI programme deemed relevant by the dutyholder?

Table 7: Examples of reporting types and intelligence users

Reporting Types	Intelligence User			
	All Staff	Technical Teams	IT/Sy Managers	Executives
Adversary Country Profile (high level intent and capabilities, including constraints)	No	Yes	Yes	No
Alerts (highlighting adversaries' TTPs)	No	Yes	Yes	No
Annual Reports	No	Yes	Yes	No
Anomalous Account Behaviour	No	Yes	Yes	No
Anomalous Device Activity	No	Yes	Yes	No
Anomalous Network Activity	No	Yes	Yes	No
APT profiles (group intent, targeting, tools, tactics and techniques, behaviour)	No	Yes	No	No
Brief Intelligence Report (highlighting singular important changes in the threat environment; for instance, around Phishing)	Yes	Yes	Yes	No
Executive Brief	No	No	Yes	Yes
Government Briefings	No	Yes	Yes	Yes
Government Technical Advice	No	Yes	Yes	No
Government Reports	No	Yes	Yes	Yes
Industry Sharing Reports	No	Yes	Yes	No
Internal Incident Reports	No	Yes	Yes	No
Internal Security Product Reports	No	Yes	No	No
Strategic/Sector specific (illustrating threats from states, criminals, hacktivists, terrorists and insiders)	No	Yes	Yes	Yes
Technology trends (i.e., Cloud computing, UAS developments)	Yes	Yes	Yes	No
Threat Feeds	No	Yes	No	No
Threat-informed scenarios for penetration testing	No	Yes	Yes	No
Vulnerability Reports	No	Yes	Yes	Yes

Appendix 3: The Principles of Intelligence

1. Intelligence at all levels is guided by enduring principles which should govern the mind-set, organisation and activities of those involved [26]. CREST summarises the principles that intelligence processes and products should adhere to [28]. It is based upon the Verisign CROSSCAT-V model, as laid out in Table 8, and is used as guidance for establishing a formal TI capability [37]. Reference [26] provides a broadly similar set of principles with nuances around the protection of sources of information and offers; Perspective – 'getting inside the mind-set of key actors; particularly adversaries' to think like them; Agility – as an ability to exploit information in context 'at the right tempo' to be forward leaning in identifying threats and opportunity; and Collaboration – as a 'duty to share' product as well as protect the information.

Table 8: CROSSCAT-V guidance for establishing a formal TI capability

Principle	Description
Centralised Control	A single point of control for intelligence team simplifies interactions and eliminates duplication of effort.
Responsive	The team must answer the question the customer asked, not the question the intelligence team wishes to answer.
Objectivity	An intelligence team should not pick sides, no matter how emotive a subject. (Intelligence should be unbiased, undistorted, intellectually honest and free of prejudice).
Sources & Methods Protection	Sources of information (both human and non-human), an organization's technical capabilities and its operational methodologies are the lifeblood of an intelligence team – and must be protected.
Systematic Exploitation	Intelligence is a methodological practice of research and review, using multiple sources and agencies.
Continuous Review	Intelligence has a shelf life, and the intelligence team must carry out a periodic review of their product to ensure it remains relevant.
Accessibility	An intelligence team must constantly balance the risk of its product falling into the wrong hands with the need for the customer to access that product.
Timeliness	Delivering intelligence products to customers in a timely fashion is central to the intelligence function.
Vision	The intelligence team must consider possibilities that are not immediately obvious. Often, the vision of an intelligence analyst, combined with the moral courage to voice an unconventional theory in an open forum, can make the difference between operational failure and mission success.

Inspectors should consider

- Does the dutyholder demonstrate adherence to defined principles of intelligence within their TI processes, and are these formally recorded as underpinning guidance?