Countering The Threats From Uncrewed Aerial Systems

A Guide To Selecting C-UAS Technology

Published: April 2023
Classification: Official

National Protective Security Authority

Contents

Executive Summary

This guidance sets out the steps that sites should undertake to deliver C-UAS technology.

Multiple types and combinations of C-UAS technology are available for purchase, and their performance varies considerably. It is critical that the performance of the equipment selected is understood, matches the site's needs and complies with the law.

The five steps described are intended to ensure that the most appropriate equipment is selected.

Step 1 – Details the need to develop a clear set of Operational Requirements (OR).

Step 2 – Provides information on how sites can use the NPSA Catalogue of Security Equipment (CSE) to select C-UAS technology.

Step 3 – Highlights the need for a robust in-situ test plan.

Step 4 – Details the need to ensure that as the technology enters live operations:

- The necessary plans, policies and standard operating procedures are in place and integrate effectively with other aspects of site operations and stakeholder planning.
- Training is delivered.
- Testing and exercising takes place and key stakeholders are involved.

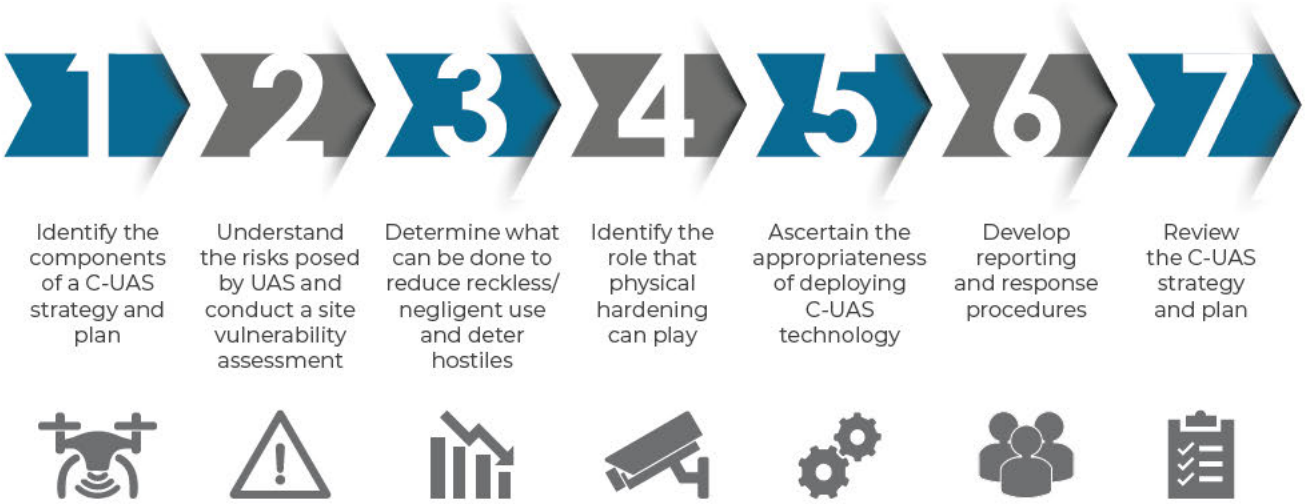
Step 5 – Sets out the need to make certain that the technology deployed remains effective:

- An assurance plan is developed to confirm that technical and operational capabilities remain effective.
- The threat is regularly reviewed, and the mitigations flex, as necessary.

The introduction of C-UAS technology is extremely complex and will require considerable resources. Before commencing detailed planning further guidance should be sought from a NPSA adviser.

An Introduction To C-UAS Technology

This guidance builds on the framework and guidance set out in the document titled Countering Threats From Uncrewed Aerial Systems - Making Your Site Ready and the other supplementary guidance documents, as described in the document titled – Countering Threats From Uncrewed Aerial Systems – guidance document structure.



Only once the steps described in section 1 and 2 have been taken, and it has then been established that the operational measures are not sufficient and that the residual risk is unacceptable should a site start detailed planning for C-UAS technology.

This guidance provides information on:

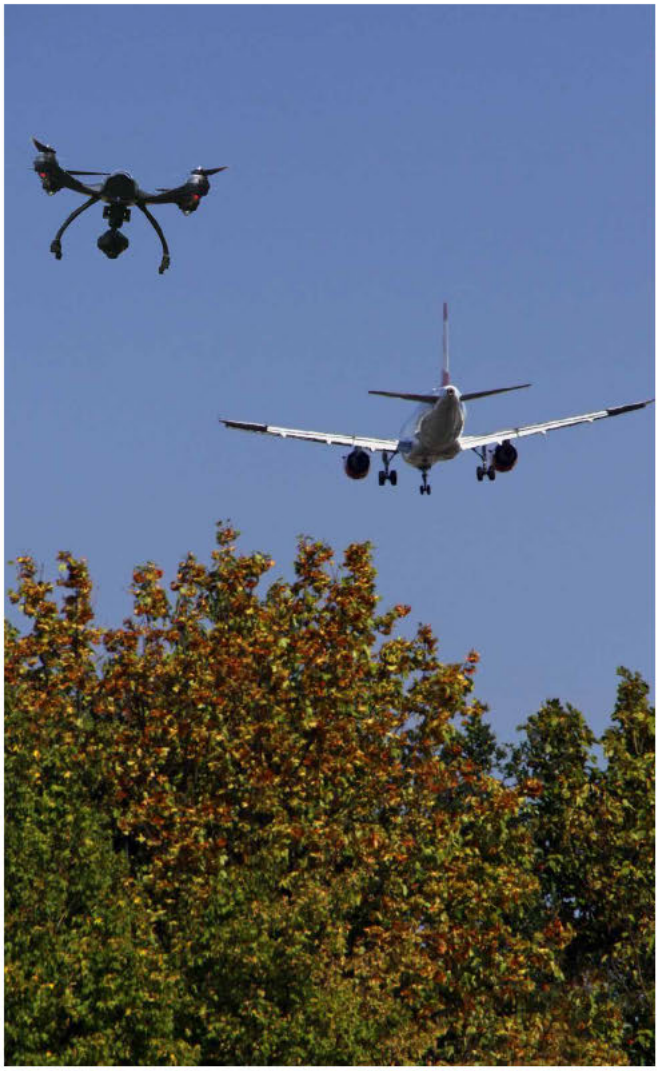
1. How the C-UAS strategy and plan will inform the selection of technology.
2. How the information gathered through the C-UAS Vulnerability Assessment (VA) will help determine the requirements for, and use of, the technology.
3. The need for developing a site-specific technical operational requirement (OR).
4. How the NPSA Catalogue of Security Equipment and NPSA C-UAS standard should be used to inform the design and procurement of C-UAS technology.
5. The need for in-situ testing to prove the system chosen works.
6. Moving to live operations.

Additional information is provided in other NPSA guidance documents in relation to many of the detailed tasks that need to be completed.

As UAS use has increased there has been a corresponding rise in unauthorised use. In response to this there has been a significant increase in the development of C-UAS technology. The purpose of following the steps laid out in this guidance is to reduce the risk of sites purchasing C-UAS technology that simply does not deliver what is needed.

Following the steps defined in this document is intended to result in the introduction of C-UAS technology that:

- Performs to the level required.
- Meets the specific requirements of the site.
- Mitigates the risk that are manifested at the site.
- Meets the NPSA C-UAS standards.
- Delivers the anticipated level of performance.
- Is cognisant of UK law.



C-UAS Strategy And Plan

Once a decision is made that C-UAS technology is needed, it is essential to recognise how the strategy and plan will be used to inform the choice of technology. The site's C-UAS strategy and plan will contain information that will help shape the configuration of the technology. A C-UAS strategy will set out the broad issues in play, the vision for the primary mitigations and what the intended effect or outcome of these will be. The C-UAS plan will build upon the complex range of mitigations and ensure that they deliver both initial and enduring operational security capabilities.

There is a direct link between the technology chosen and the plan. The plan will describe how the information gathered by the technology will be used to protect the site. For example, the type and level of reliability of the information that the technology gathers about a UAS will be used to inform operational decision making. There is little value in introducing C-UAS technology, producing valuable information about the UAS activity at a site, unless there is a plan as to how the data produced will be used.

Identifying Vulnerabilities And Understanding The UAS Risk

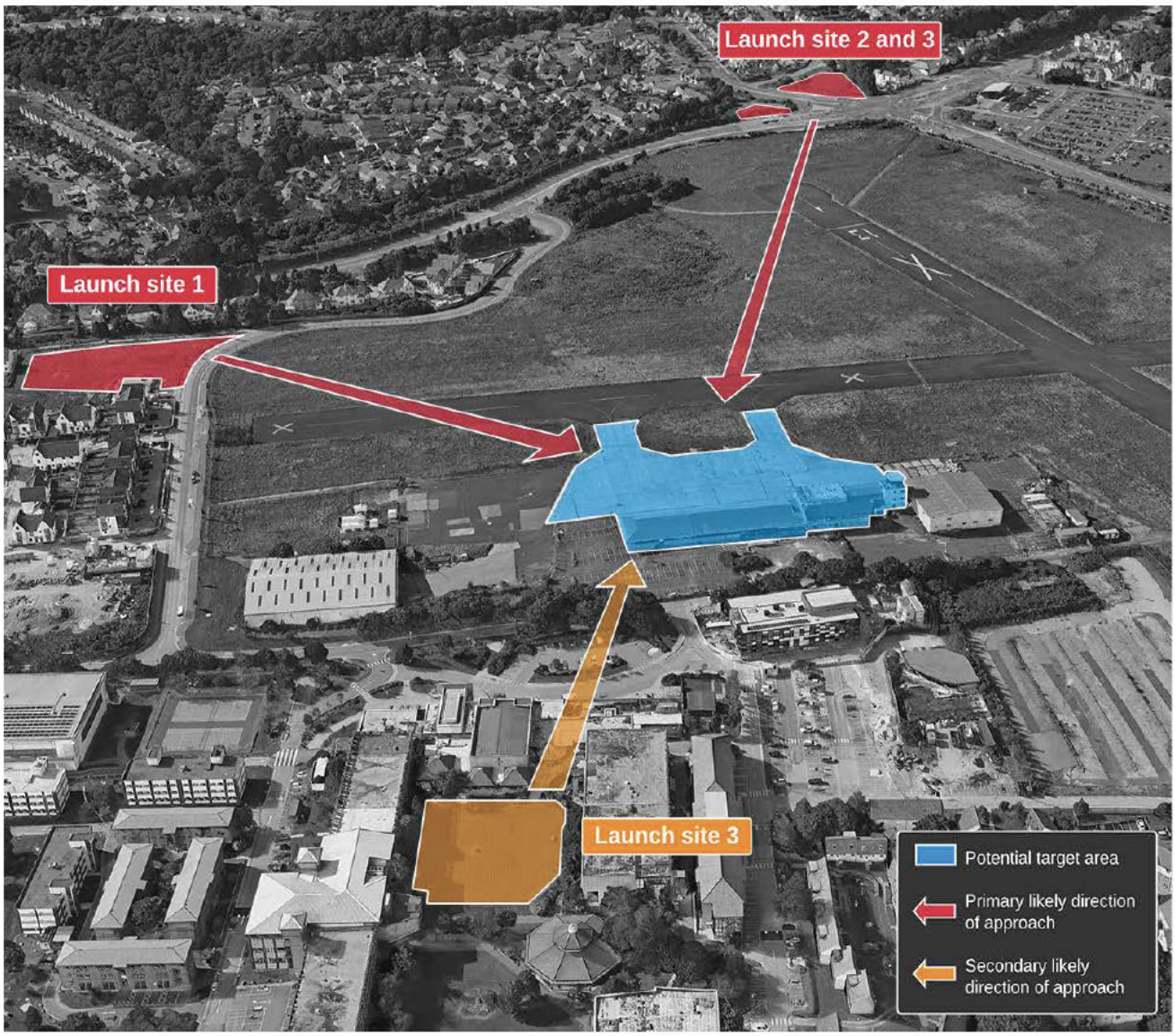
The C-UAS Vulnerability Assessment (VA) for a site is intended to establish:

- The key assets vulnerable from a UAS.
- The UAS threat actors and scenarios considered relevant to the site.
- The protection offered by existing mitigations.
- The most likely potential launch sites and flight paths.

The information gathered can be used to inform:

- The understanding of the threat and risk from UAS to a site.
- Decisions regarding the potential need for additional C-UAS mitigations.
- The requirements for C-UAS technology.
- The response procedures triggered in the event of a suspected intrusion.

The VA process should be completed before a decision is made as to whether C-UAS technology is required.



Introduction To C-UAS Technologies

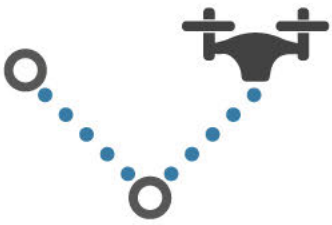
Types of C-UAS technology

The C-UAS technology market is expanding rapidly but is still relatively immature. It is therefore important to make sure, that as sites are considering the installation of a new technology that at an early stage within this process, guidance is sought from a NPSA adviser.

C-UAS technology is broadly split into two primary types. The first type of C-UAS systems are intended to detect the presence of a UAS, track and identify it (DTI). The second type are intended to support or deploy measures (effectors) to disrupt and mitigate its effect (E). As a result of the legalities and safety considerations associated with deploying effectors in an operational environment, E solutions, whilst mentioned above, are not expanded on further within this document at this time.

DETECT

The ability to sense and classify the presence of a UAS.



TRACK

The ability to determine the UAS position and movement over time.

IDENTIFY

The ability to determine the size and type (fixed wing, multirotor) of a UAS.

EFFECT

Using a technical effect to prevent the UAV from completing its intended activity

There are several different C-UAS DTI technologies currently available on the market and under development. These are:

RADAR SENSORS

Transmits pulses of radio waves and receive the reflection of those waves from objects in their path.

RADIO FREQUENCY SENSORS

Detects radio frequency signals emitted.

ACOUSTIC SENSORS

Detects sound waves emitted.

ELECTRO-OPTICAL SENSORS

Visual and infrared cameras receive photons from the scene being viewed and convert them to electrical signals and produce images.

The purpose of introducing C-UAS technology is to:

- Deter hostile UAS activity.
- Provide an early warning of an unauthorised UAS approaching a site.
- Provide rapid and reliable detection of a UAS within a designated area (e.g. a site).
- Provide reliable information that will clarify the situation, inform decisions, including those relating to operational and technical responses.
- Inform wider decision making as to the safe and secure operation of the site as the incursion is being investigated.
- Support the investigation into the intrusion, including both evaluating the residual risk of the intrusion and evidential capture to assist with the identification or prosecution of the perpetrator.

A DTI solution may be comprised of a number of different sensors and technology types, that may be technically integrated to improve the overall effectiveness of the solution. [1]

Before commencing a project to introduce C-UAS technology at a site, important information must be gathered. These steps are described in our other guidance documents and include:

- Developing the C-UAS Strategy and plan [2]
- Completing the vulnerability and risk assessments [3]

Detailed guidance into the content of the C-UAS technical OR is available in the document titled: Countering the threats from Uncrewed Aerial Systems - Developing Operational Requirements for C-UAS Detect, Track and Identify technology.

[1] Further detail on different types of DTI technology is available in Introduction to C-UAS technologies for use in homeland security applications

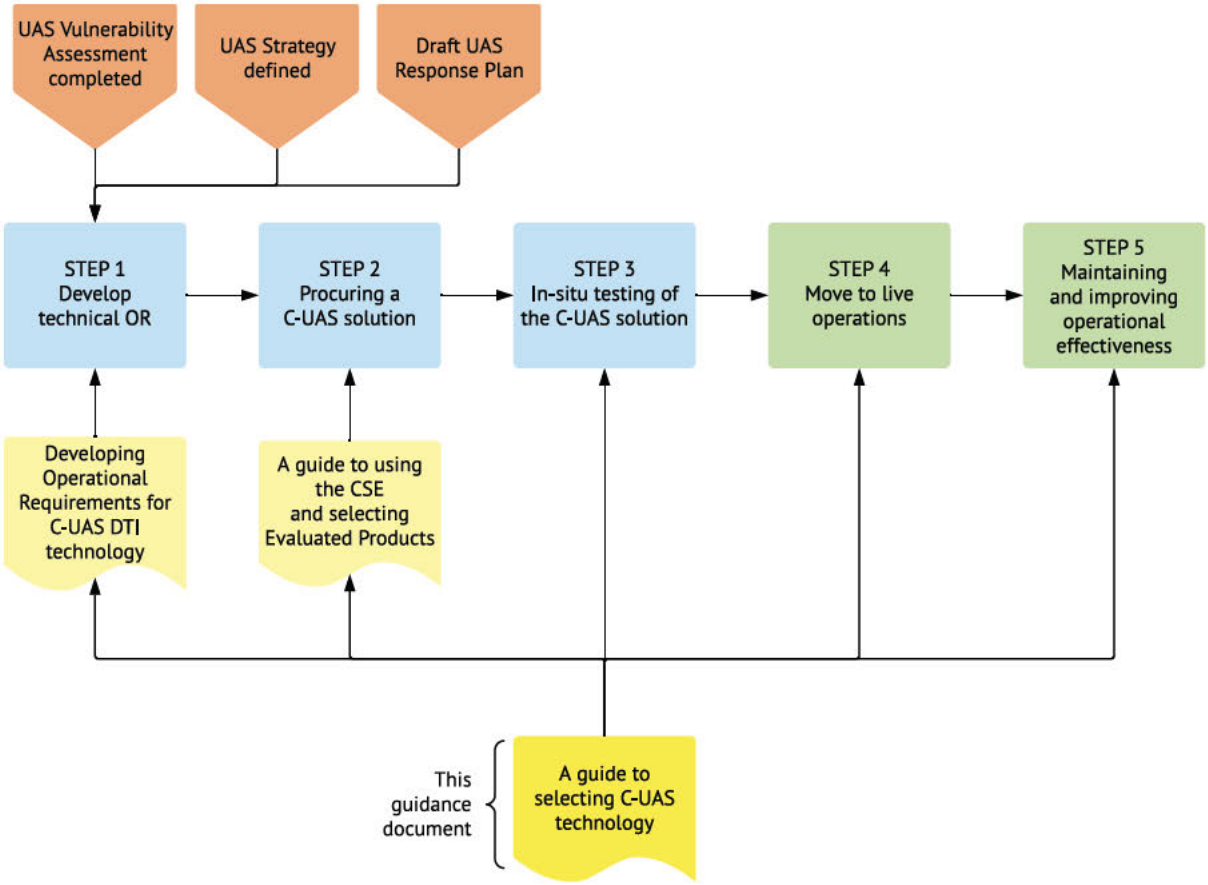
[2] Countering threats from Uncrewed Aerial Systems - Developing a strategic approach

[3] Countering threats from Uncrewed Aerial Systems - Developing Operational Requirements for C-UAS Detect, Track and Identify technology

The information gathered will be used to inform the procurement of C-UAS technology. Following this process should ensure that the C-UAS equipment selected will:

- ☑ Match the objectives defined in the C-UAS strategy.
- ☑ Provide mitigation against the identified risks.
- ☑ Integrate with the existing technical and operational security capabilities.
- ☑ Enable a more effective response to any suspicious UAS incident.
- ☑ Support the overall safe and secure operation of the site.
- ☑ Deliver technology of proven capability.

There are five main steps that should now be completed. An introduction to these steps is provided below. Detailed information is provided in the relevant supplementary documents.



There is an opportunity to seek approval from the appropriate decision maker within the site's senior leadership as each step is completed. Agreement should be sought that the work completed reflects the site's strategy and needs, and that the organisation is willing to progress to the next step in developing the C-UAS technical solution.

Detailed guidance into the content of the C-UAS technical OR is available in the document titled: Countering the threats from Uncrewed Aerial Systems - Developing Operational Requirements for C-UAS Detect, Track and Identify technology.

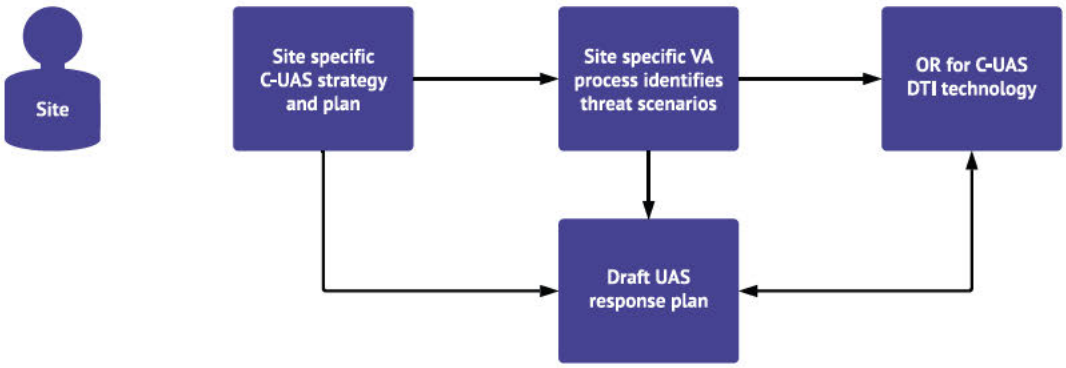
Step 1 - Develop A Site Specific Technical OR For C-UAS

NPSA recommends the OR process for the development of protective security solutions. The process will make use of a considerable amount of information that has already been gathered.

Once a high-level statement of requirement has been produced and agreed, it is necessary to gather a comprehensive set of requirements; these will be used to inform the detailed design of a C-UAS technical solution. The process will ensure that all aspects of the C-UAS threat, operating environment, legal and security constraints are considered as a solution is procured, designed and taken into live operation. Following the guidance and answering the questions provided should result in the information gathered being in a format that can be easily understood by those involved in the specification and procurement process.

Examples of environmental issues:

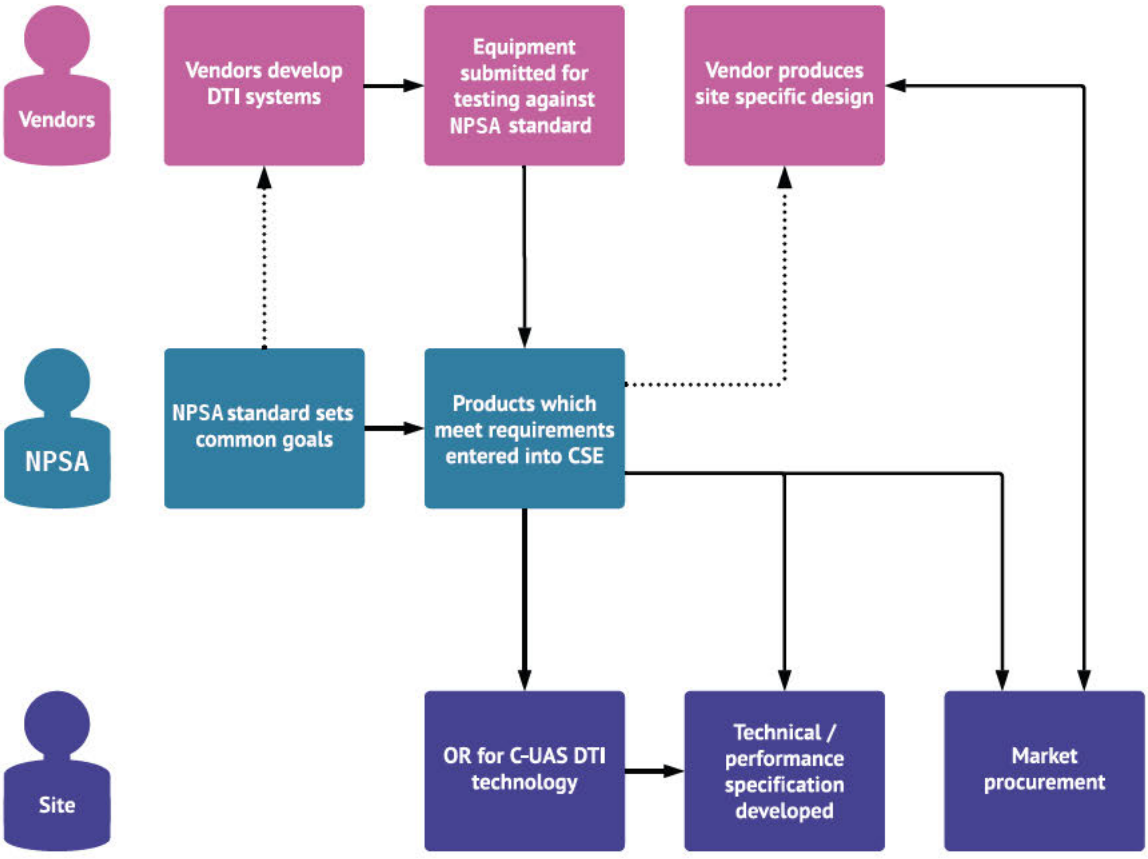
- Topography, causing line of sight issues
- Large buildings/features, water, vegetation that may interfere with radio waves
- Presence of transmitters
- Identification of equipment that may be interfered with by certain type of DTI system (e.g. radar)
- Off-site locations where privacy may be an issue and appropriate steps need to be taken (e.g. long range cameras)



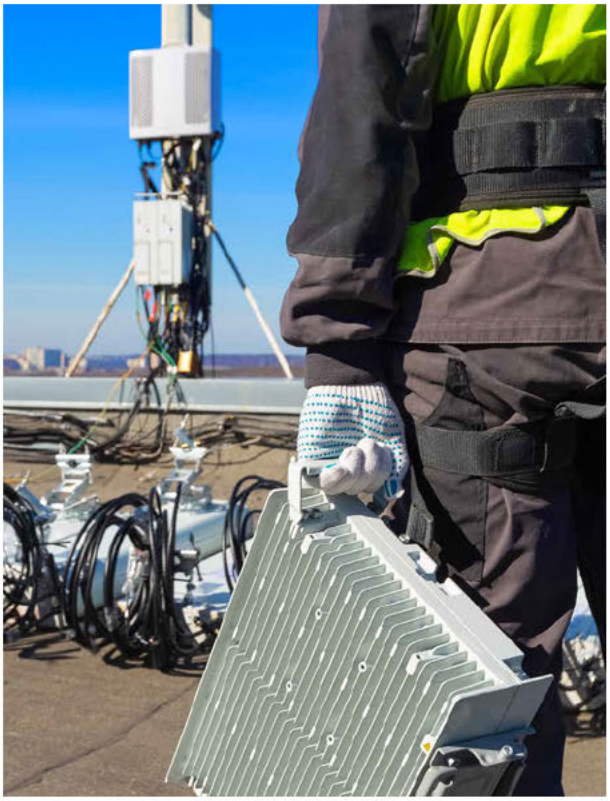
Step 2 – Developing Detailed Design And Procuring C-UAS Technology

Matching the CSE against the OR for C-UAS technology

When all the essential information has been pulled together into the OR and answers are provided to the questions, the information may be used to identify potential solutions contained within the Catalogue of Security Equipment (CSE), appropriate for your site.



The design and build phases will take the system from an outline design, through detailed design and into the start of testing, including Factory Acceptance Testing (FAT) before installation onto the site. Equipment should be tested in a controlled factory environment, ensuring that the system and each component is working correctly and meets the standards defined within the procurement process.



Consideration could also be given to a managed services or equipment rental arrangement. This approach would mitigate the complex risks of installing and operating C-UAS equipment by placing some of the responsibility on the supplier. This may prove beneficial at a time of rapid developments in technology and threat.

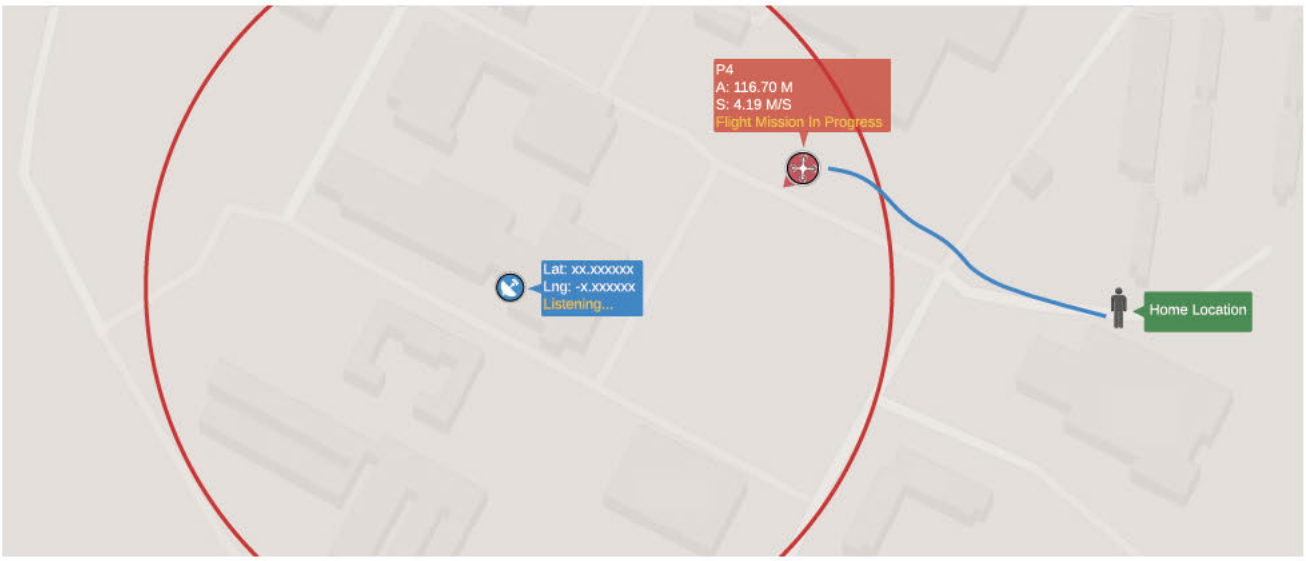
Detailed engagement will be required between the site, manufacturers of the selected systems and subject matter experts to further understand the suitability of different systems for use at a site. The NPSA CSE should not be viewed as a catalogue for purchasing technology without engagement with NPSA advisers, manufacturers, system integrators and independent experts, as this helps to ensure that the most appropriate technology and system(s) are being chosen for use at each site.

Step 3 – Installation And In-Situ Testing

Step 3 is the first of three steps that cover the transition into live operations and the handover of the equipment to the site.

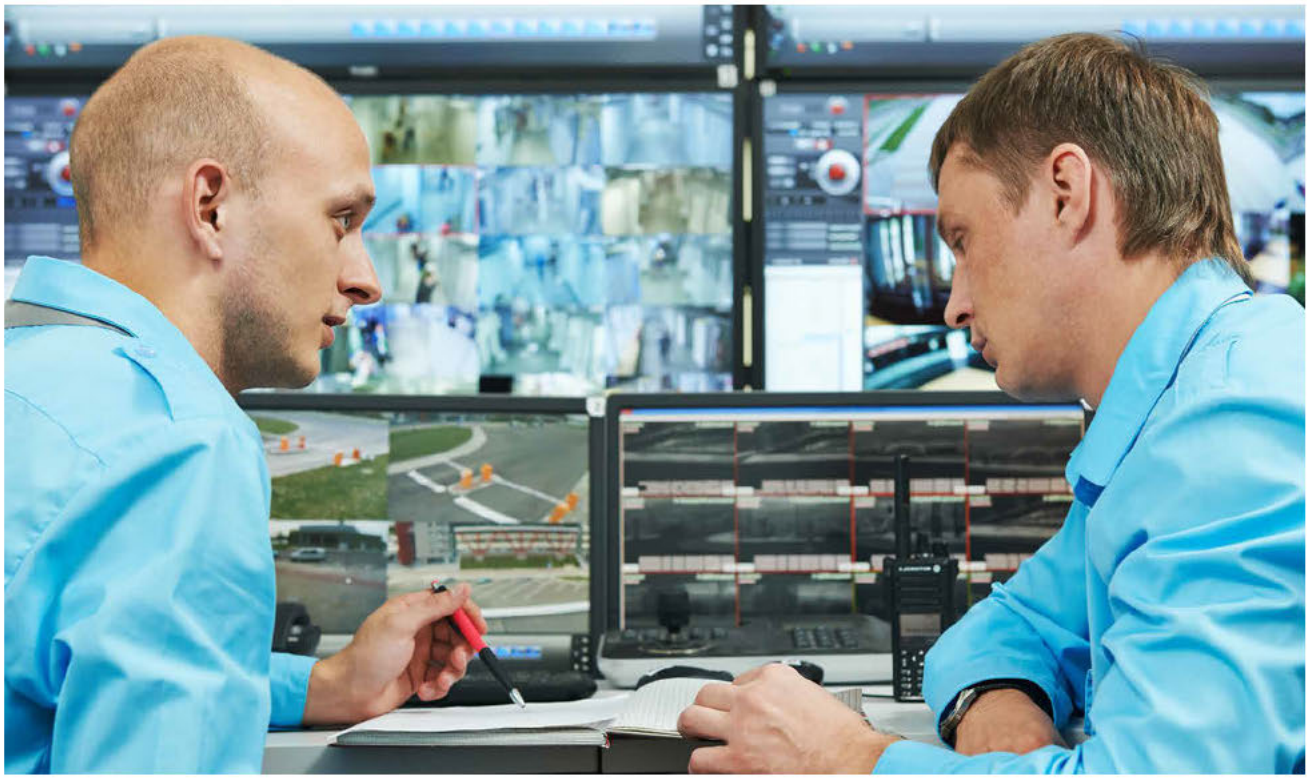
Despite diligent design and factory testing of equipment, the real world siting and deployment of the kit is likely to impact on its performance and these issues will need to be identified and resolved. For this reason, during the installation period, the system should go through a series of tests.

This period of testing is intended to ensure that the system as deployed on-site meets the performance levels defined within the OR and enables the C-UAS mitigation strategy to be fulfilled. In-situ testing is complex and needs to be undertaken by competent persons in a methodical way. Due to the critical nature of this phase of delivery, NPSA recommends that commissioning tests involve an independent third party, reporting directly to the client.



During this stage it will be necessary to make certain that the appropriate training is provided to the operators who will be using the equipment. Training should cover:

- Equipment training, enabling operators to use the equipment.
- Training on site operating procedures (SOPs) that will set out how the information generated by the technology will be used to inform an operational response.



A detailed test plan will ensure the following:

- ☑ That each component works on its own.
- ☑ All the components of the system work together.
- ☑ The whole system integrates effectively with the other technical systems.
- ☑ The system is secure and legal to operate.
- ☑ There is an understanding of the unintended consequence of using the system in or near to the site.
- ☑ The operational policies and procedures work effectively with the new technology.
- ☑ That appropriate training is in place.
- ☑ The OR has been met.

Step 4 – Moving To Live Operations

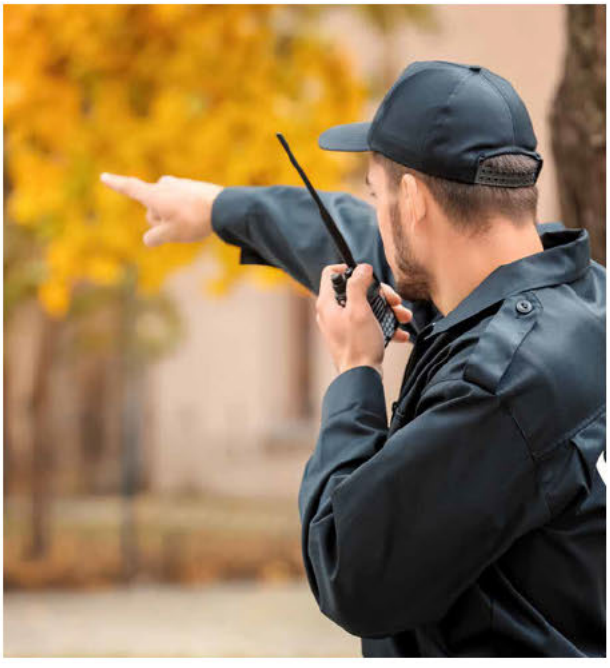
C-UAS technology is likely to be one of the most complex technical security solutions deployed within a site. The DTI technical equipment introduced will be present to improve the situational awareness of those within the SCR and provide critical information that will be used to inform decision making. When a detection is made, there will be very little time for the SCR to seek authority before action is taken. It will, therefore, be essential that there are carefully thought out plans, policies and standard operating procedures that support the deployment of DTI equipment. This period will focus on ensuring the capability is operationally effective.

The following plans should be either reviewed or developed in response to the introduction of C-UAS technology:

- Response plans that cover the following key tasks, identify the stakeholders to be engaged and the communication methods used during:
  - Incident Response (IR)
  - Incident Management(IM)
  - Crisis Management (CM)
  - Business Continuity and Resilience (BC)
  - Business Recovery (BR)
- Information security plan
- Maintenance/servicing plan
- Contingency plans covering equipment failure and a rapid change in the threat.

Detailed guidance is available from NPSA to support sites planning to respond to an incident in the following documents:

- Responding To Terrorist Incidents - Developing Effective Command and Control
- Communications Technology - Interim guidance to assist organisations prepare for a terrorist incident



Testing and Exercising

A detailed testing and exercising plan should be developed. This will be used to ensure:

- That the technology that has now been installed and the plans that have been developed are effective.
- The roles and responsibilities of the key internal and external stakeholders are fully understood. This will include engagement with the local police force to make certain that there is a shared understanding of the response they will provide.

Information security

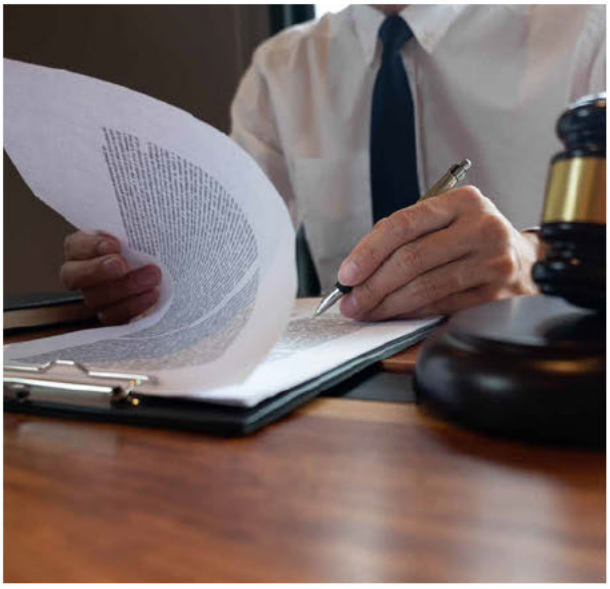
The deployment of technical C-UAS measures is likely to deter attackers from flying a UAV at a site as they will fear that they will either be caught, or the attack frustrated as a result of the deployment of a sophisticated technical security measure. However, the precise details of the capability provided by any C-UAS technology deployed should be closely guarded and not released into the public domain. Further information is provided in relation to deterrence communications in the NPSA document titled Security-minded communications for Countering Uncrewed Aerial Systems (UAS).

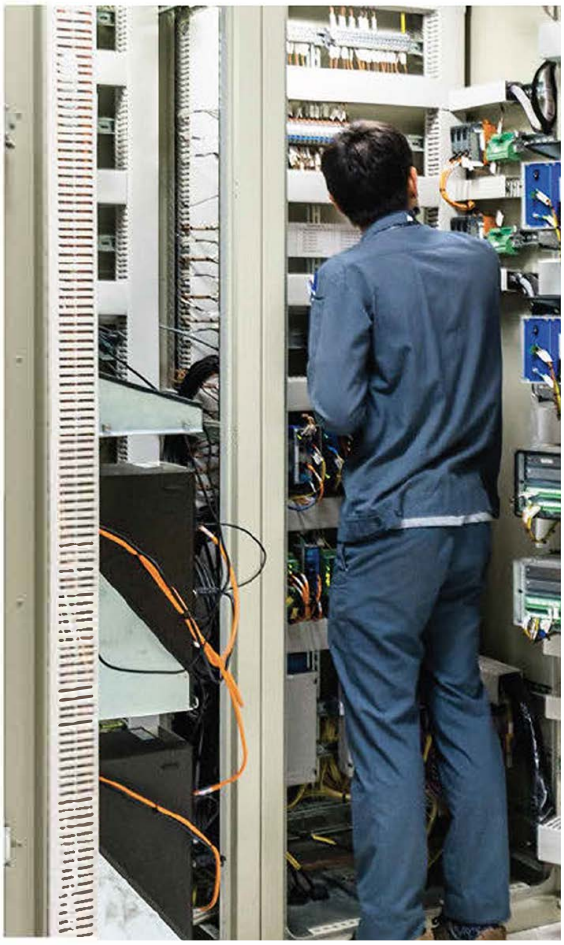
When responding to an incident or releasing information to the media about the security plans in place, detailed information should not be supplied as to the type or capability of the equipment. Only the most informed adversary is likely to be able to identify through hostile reconnaissance the type and performance of any measures deployed.

Detailed and sensitive information may be shared with the companies involved in supplying and supporting other aspects of a project to deliver C-UAS technology. Careful consideration must therefore be given to security within the supply chain. Detailed guidance in relation to supply chain security is available from NPSA. For more information search NPSA – Supply Chain.

Compliance

It is the responsibility of the equipment purchaser and the supplier to ensure that any system is suitable for each deployment and that it complies with all legislation, standards, codes of practice and other relevant requirement. Therefore, prior to procurement and deployment detailed guidance should be sought from a site's legal advisers to confirm a system's compliance. Legislation to consider includes, but is not limited to, the Data Protection Act 2018, the Investigatory Powers Act 2016, the Wireless Telegraphy Act 2006 and the Computer Misuse Act 1990.



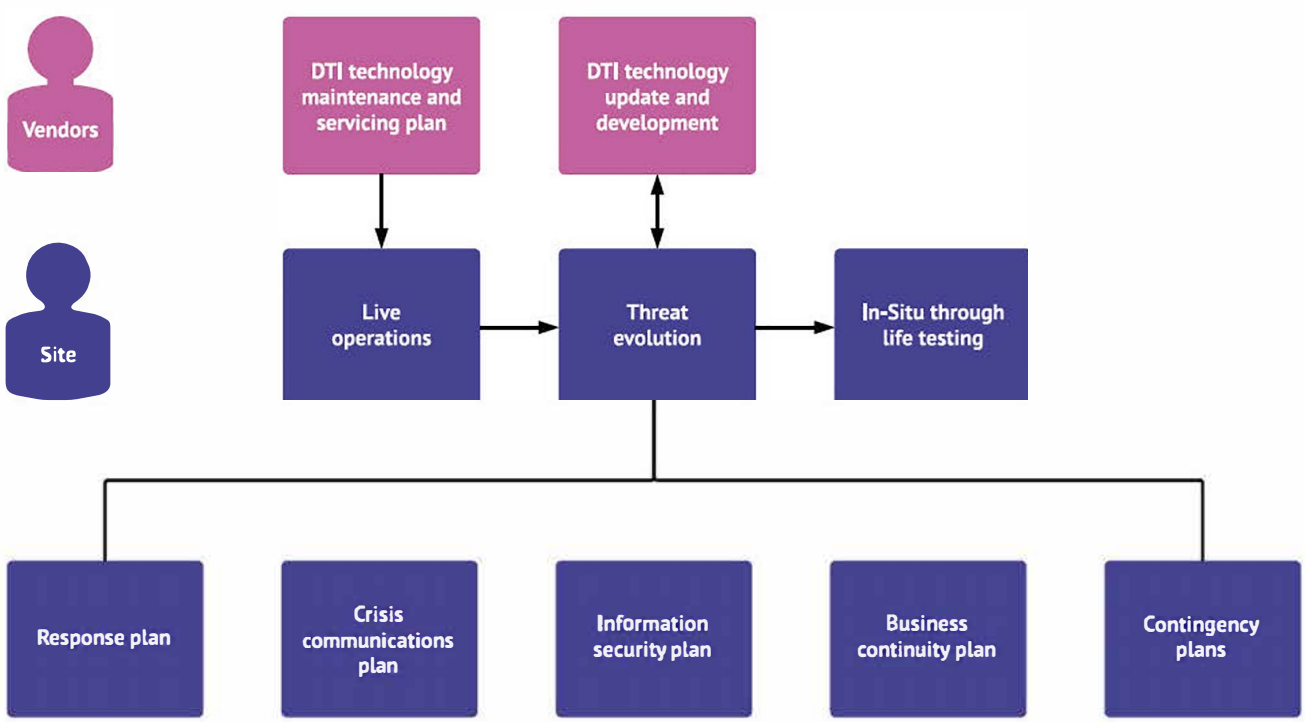


Equipment updates and servicing

As a result of the continuing development in the technology and developments in the types of UAS that are available it will be important to make certain that the DTI technology can be updated as required.

Sites must be confident that the equipment installed remains serviceable and that, in addition to regular checks being completed to make sure it is working, there is a servicing contract in place. Checks will ensure that both the software and hardware is working effectively and, where necessary, updated.

The UAS threat will continue to develop and it may be necessary for the system to adapted to ensure that it can respond to the evolving threat and changes in the response procedures. As such changes are made a further period of detailed testing will be necessary.



The response to any system fault should be on a timely basis, as set out within the technical requirements document and agreed through the contract. The intention should be to reduce the time that the system is either down or operating incorrectly.

Step 5 - Maintaining And Improving Operational Effectiveness

Review

A regular review should be completed of the VA. Reviews should consider changes in the UAS threat and continuing developments in the capability of both the UAS and C-UAS technologies which could significantly change the level of risk.

Post incidents reviews should take place after each significant incident. These should consider how the technology worked to detect the potential threat and inform the operational response and investigation into the incident. It is important to make sure that the best use was made of the information that the technology provided.
Information should be gathered as to the effectiveness of the C-UAS technology in operation, and the site should work with the vendor to improve subsequent performanee.

Assure

Once the equipment has moved into live operation, an assurance plan should be developed to make certain that the equipment continues to deliver the capability required. The assurance plan should confirm the following:

- The equipment continues to work effectively
- Staff and management have the necessary training
- The policies and procedures are up to date.

A testing and exercising plan should be developed The purpose of this will be to make certain that all elements of the response plan remain effective and is appropriately integrated with key internal and external stakeholders.

Summary

The decision to procure C-UAS technology is a complex one. It must factor in:

- The risk of unauthorised UAS activity occurring at the site.
- An understanding of the benefit technology will deliver in managing an incident.
- The selection of the most appropriate system.
- How the system will fit within the overall protective security operation of the site.
- The legal issues associated with the deployment of the equipment.

Resources must be made available to make sure that all the steps are completed on a timely basis.

It is essential to recognise that the capability and performance of both UAS and C-UAS equipment are changing rapidly. Additional information is available from the NPSA extranet that provides guidance in relation to:

- The overall approach to C-UAS planning.
- The development of a Vulnerability Assessment.
- The development of an Operational Requirement for C-UAS technology.
- The testing and evaluation of C-UAS technology.
- Reporting and responding to UAS incidents.

Consideration should also be given to approaching similar sites around the country who have already procured C-UAS technology, requesting that they share the lessons they have learnt from delivering a similar project.

The C-UAS guidance is being updated on a regular basis. Before commencing detailed planning, the extranet should be checked and advice should also be sought from a NPSA adviser to make certain the most up to date advice is available.

Annex A - Types of Specification

Performance specification

A performance specification will describe the outcome that the technology is intended to deliver. This would include items such as:

- The height and range covered by detection zones
- The UAS components (UAV and/or GCS) to detect
- The level of precision required in identifying the position of the UAS
- The number of UAS
- The number of operators required.

Advantages of performance specifications:

Provide opportunity for innovation; allow bidders to present unique and innovative solutions to defined needs from equipment within the CSE.

- Allows the end user to benefit from the latest products and technologies.
- Corrective action may be applied if service levels are not achieved.

Disadvantages of performance specifications:

- Well-defined performance metrics are needed to ensure that the specified performance will achieve the desired outcome.
- Require reliable, practical, economical tests of performance.
- Evaluations are subjective and require additional time and effort to complete.

Technical specification

A technical specification will be more prescriptive and will set out in detailed terms the technical detail of what the supplier is required to supply and how it should be configured.

Advantages of technical specifications:

- Provide increased certainty about the type of solution delivered.
- Should enable a direct comparison during the evaluation of offers.
- Award is based on compliance with the specification.

Disadvantage of technical specifications

- Prescriptive, may limit competition.
- Increased risk to the organisation of needing to identify the correct design solution.
- Loss of innovation in developing the solution.
- Technical specs require considerable expertise to write, they are likely to require the services of engineers, architects, and other technical resources, as well as multiple levels of review and approval.