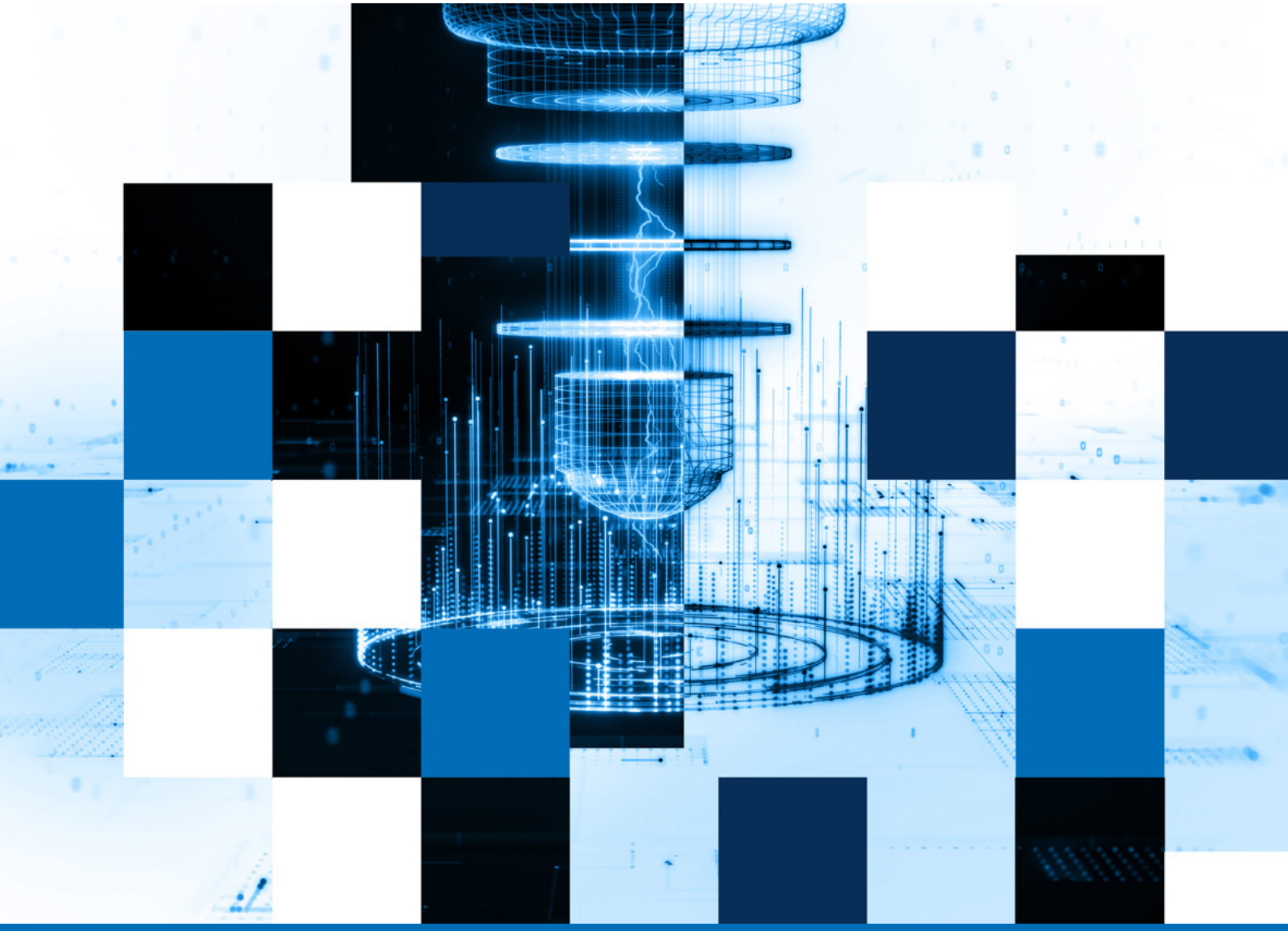
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Quantum technology primer: Sensing

For cyber security leaders



Introduction

Quantum sensing leverages quantum phenomena to make sensitive observations of activity in the physical world. It has the potential to enhance current technologies and likely allow more precise and effective measurements. Examples of measurements could include time, pressure, gravity and magnetic fields. It could also enable new sensor technologies and measurement capabilities.

This guidance is part of a series of quantum technology primers for cyber security leaders. To learn more, refer to cyber.gov.au/quantum

About quantum sensing

A sensor detects or measures a physical property that can be used to understand the physical world. Quantum sensors utilise quantum mechanical phenomena such as superposition, entanglement and shifts in atom energy level to measure physical quantities. This enables ultra-precise measurements of time, pressure, gravity, or magnetic fields.

Industries such as mining are already exploring the potential of quantum sensing for applications like subsurface imagery and resource detection. As with all technologies that have valuable information or capabilities, organisations should utilise best practice cyber security principles when integrating quantum sensor capabilities.

The impact on cyber security

Quantum sensing has the potential to provide new ways to measure and understand our physical environments in many fields. It could disrupt industries such as navigation, resource exploration, telecommunications and defence. It will build upon current technologies and will likely allow more precise and effective measurements for some use cases.

A prominent example of uses for quantum sensors is for effective navigation when GPS (Global Positioning System) is unavailable. Organisations should consider monitoring quantum sensing advancements relevant to their industry and potential cyber security risks.

Cyber security risks

Quantum sensing introduces a range of considerations for cyber security leaders, including integration and data management challenges. This highlights the importance of careful planning and protection when deploying within digital environments. Similar cyber security principles apply just as they do in other operational technology deployments.

Below are some potential risks that organisations should factor into their cyber security plans and posture.

Sensor integrity and tampering

Quantum sensors are highly sensitive and precise, but may be vulnerable to external noise. It may also be difficult to limit inputs to only the specific use cases required.

Like other sensors, organisations should manage appropriate controls, mitigations and security considerations for the location where they deploy sensors. Particularly in high-risk environments.

Data authenticity and spoofing

Like other sensors, quantum sensors may be vulnerable to spoofing attacks. A malicious actor may mimic legitimate signals or introduce unwanted noise to manipulate sensor outputs.

Organisations should consider employing mechanisms to verify the authenticity of sensor data. This may include investing in secure signal validation and anomaly detection systems.

Supply chain risks

While most quantum technologies currently rely on classical components, their unique application of quantum phenomena can introduce new vulnerabilities. Quantum technologies may depend on specialised materials or vendors. The associated hardware and firmware could be prone to tampering, counterfeit parts or malicious implants.

Organisations should consider measures such as hardware provenance, digital attestation and secure boot mechanisms for supply chain integrity. It is important to assess vendors for secure development practices and require transparency across the supply chain.

Software and firmware vulnerabilities

Like all digital systems, quantum sensors rely on software and firmware that may contain exploitable vulnerabilities.

Organisations should ensure secure development practices, regular patching, and vulnerability assessments for all quantum sensing components.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website
https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre