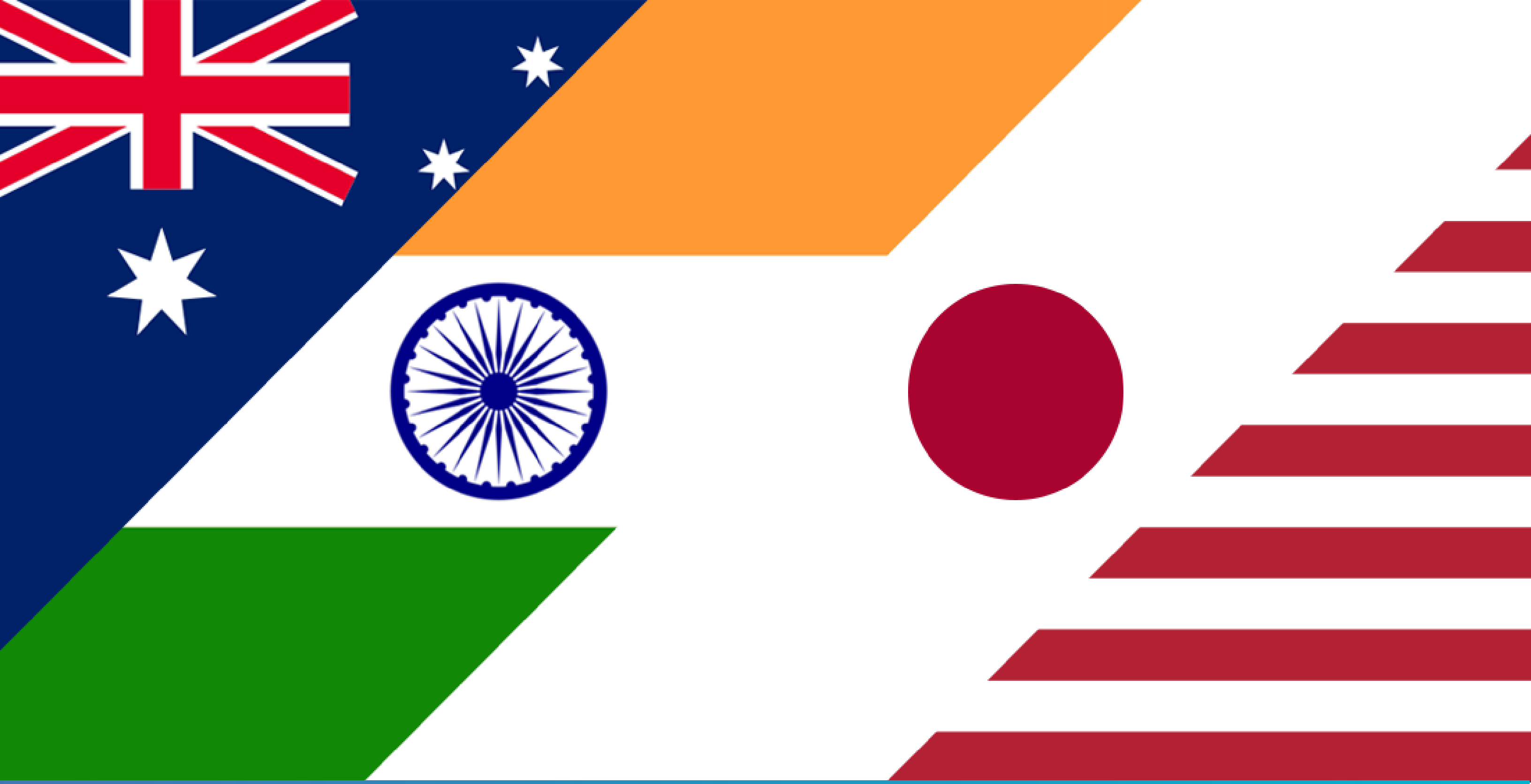

Quad Cybersecurity Partnership: Joint Principles for Secure Software

The Quad partners recognize the security risks posed by lack of adequate controls to prevent tampering with the software supply chain by adversarial and non-adversarial threats. By leveraging the voice of the Quad, we can promote and strengthen a culture where software security is by design and default. We encourage other nations to adopt these principles in pursuit of this shared vision for secure software.

The Quad Senior Cyber Group reaffirms our commitment to collectively improve software security by establishing minimum cybersecurity guidelines for governments to guide their development, procurement, and use of software. In order to implement these guidelines, where necessary, each Quad country intends to build policy frameworks, consistent with international obligations, domestic laws, regulations, and maturity of national cyberspaces. Quad partners are committed to implementing rigorous and predictable mechanisms to ensure software products function securely and as intended, and will engage with the software industry to promote these practices. By integrating secure software practices throughout the software lifecycle, the goal is to significantly reduce the number and potential impact of software vulnerabilities.

The Quad intends to pursue the following high-level secure software **development** practices and to adopt them into existing government policy, acquire software that meets these practices, and encourage software developers/suppliers to implement them:

1. *Prepare the Organization*: Ensure that people are adequately trained, processes are defined, and technology solutions are in place to perform secure software development.
2. *Protect the Software and Software Development Environment:* Ensure appropriate controls to protect all components of software from tampering and unauthorized access, archive and protect each software release, and maintain adequate records of the details (e.g., Software Bill of Materials) and supply chain relationships of the various components used in each release.
3. *Produce Well-Secured Software:* Produce well-secured and tested software with minimal security vulnerabilities in its releases.
4. *Respond to Vulnerabilities:* Identify vulnerabilities in software releases and respond appropriately to continuously address those vulnerabilities and prevent similar ones from occurring in the future.

Each member of the Quad intends to pursue the following minimum guidelines for government **procurement** of software or a product containing software. Consistent with international obligations, domestic laws, regulations, and maturity of respective cyberspaces, each Quad country intends to pursue implementation of the guidelines domestically by encouraging the following practices:

1. Require self-attestation by the software producer, unless a third-party certification is provided, stating that the software's development complies with secure software development practices.
2. Encourage the software developer to report to a respective national vulnerability disclosure program that includes a reporting and disclosure process.

The Quad intends to pursue the following security measures for government software **use**:

1. Ensure adequate controls and processes to protect software and software platforms from unauthorized access and usage.

2. Ensure adequate controls and processes to protect the confidentiality, integrity, and availability of data used by software and software platforms.
3. Identify and maintain software platforms and the software deployed to those platforms to protect software from exploitation.
4. Quickly detect, respond to, and recover from incidents involving software and software platforms.
5. Strengthen the understanding and performance of humans’ actions that foster the security of software and software platforms.