Cyber Liability Insurance for Government Contractors

Cyber liability insurance is a smart risk management tool, even when it is not required by the U.S. Government.

Government contractors often handle sensitive data, rely on technology to perform contracts, and face real exposure to ransomware, data breaches, funds transfer fraud, business interruption, and third-party claims.

The value of cyber coverage goes beyond the policy itself.

It can provide access to breach response professionals, legal counsel, forensic experts, notification support, and recovery resources when a cyber event happens. That support can be critical when contract performance and reputation are on the line.

CMMC efforts can strengthen your cyber insurance profile.

While CMMC certification does not guarantee a lower premium, the security controls required for CMMC often align with what cyber underwriters want to see. This may help improve insurability, support better underwriting results, and in some cases contribute to more favorable pricing or terms.

Security measures that may positively influence cyber underwriting

The following controls are often viewed favorably by cyber underwriters and support CMMC readiness:

- Multi-factor authentication
- Endpoint detection and response
- Secure backups that are tested regularly
- Access controls and least privilege
- Employee security awareness training
- Incident response planning
- System monitoring and logging
- Documented cybersecurity policies and procedures

The stronger and more consistently these controls are applied, the better the organization tends to present to insurance markets.

Why this coverage is worth considering

Cyber liability insurance helps protect the company's balance sheet, client relationships, and ability to continue operating after an incident.

Even if the government contract does not require it, the coverage can still be valuable for protecting the business and showing customers, Prime Contractors, and business partners that cyber risk is being taken seriously.

Technology E&O should also be considered

Technology Errors and Omissions coverage is often paired with cyber liability coverage. That is because it addresses a different exposure. Cyber liability is focused on security and privacy events. Technology E&O is focused more on claims arising from a failure of the technology product or service itself.

Technology E&O may not be required by the U.S. Government, but it is often required by Prime Contractors or commercial customers.

For contractors providing IT, software, systems integration, managed services, or other tech-based services, this coverage can be an important part of the overall insurance program.

Bottom line

CMMC certification efforts can do more than support contract compliance.
They can also help demonstrate stronger cyber discipline to insurance underwriters.

Cyber liability and Technology E&O coverage can help protect revenue, preserve trust, and strengthen the contractor's position in both government and commercial markets.