Webinar Q & A: Microsoft and Exostar: Empowering Secure, Compliant Collaboration for Highly-Regulated Industries

On October 14, Microsoft's Richard Wakeman was joined by Exostar's Kevin Hancock and Joel Williams to discuss how we've joined forces to create Exostar Secure Access for Microsoft 365. Part of The Exostar Platform, the Exostar Secure Access for Microsoft 365 application empowers enterprises and their partners in highly-regulated industries by combining the ease-of-use of Microsoft 365 with an additional layer of data protection to deliver secure and compliant collaboration.

We received a lot of great questions prior to the live webinar. Here's the list of all the questions submitted with the answers. While not all of the questions were focused on Secure Access for Microsoft 365, there were some interesting DIB questions around CMMC, NIST 800-171 and DFARS that are answered below.

Q. Is this offering FEDRAMP certified and if so, to which level? Will it satisfy CMMC level 3 requirements?

Exostar's Secure Access for Microsoft 365 includes an Exostar Managed Tenant in the Microsoft environment that is required by our customers. If you are a Defense Industrial Base (DIB) customer, we will utilize the GCC High Environment. GCC High was created to meet the needs of DoD and Federal contractors that needed to meet the stringent cybersecurity and compliance requirements of NIST 800-171, FedRAMP High, and ITAR, or who need to manage CUI/CDI.

Q. "Will there be compute resources available to interact with the data residing in the Exostar Secure Access? **Personally, I have setup up several DIB members to support workloads similar to the Exostar offering. Would love to hear more about the roadmap and if Azure Virtual Desktop is on the roadmap."

With this initial release we are focused on utilizing Microsoft Teams and its real time collaboration capabilities. We do anticipate a need for endpoint protection as well an Azure Virtual Desktop may be a part of that particular solution or an additional service at a later date. Stay tuned.

Q. How is the Exostar Secure Access set up to comply with ITAR & CMMC requirements?

The managed tenant hosting the service will be established in an Azure GCC High Environment. GCC High was created to meet the needs of DoD and Federal contractors that needed to meet the stringent cybersecurity and compliance requirements of NIST 800-171, FedRAMP High, and ITAR, or who need to manage CUI/CDI.

Q. Is your collaboration environment using Exostar Secure Access for Microsoft 365 for highly-regulated industries CUI/ITAR compliant, similar to GCC-High?

The managed tenant hosting the service will be established in an Azure GCC High Environment. GCC High was created to meet the needs of DoD and Federal contractors that needed to meet the stringent cybersecurity and compliance requirements of NIST 800-171, FedRAMP High, and ITAR, or who need to manage CUI/CDI.

Q. Will it function using Microsoft Edge?

Yes, users can access Microsoft Teams utilizing Microsoft Edge so the solution will work for users that want to use Microsoft Edge

Q. Do either MS or Exostar have an immutable record system that supports data exchange between teams or supply chain partners?

Secure Access for Microsoft 365 is a collaboration tool, that allows for document collaboration in real time. It will version documents and keep records of who has made changes. Additionally, you will be able to use DLP-type products to determine users that can or cannot copy, edit, delete, or otherwise change documents in future releases.

Q. Can you send the list of security applications or addons you will be discussing? Thank you.

This was a product introduction webinar for Exostar's Secure Access for Microsoft 365. Additional information for this product can be found here, and a replay of the webinar is available here.

Q. Does Microsoft 365 meet CMMC requirements such as US based server farm, compliance with not utilizing foreign citizens for maintenance, and other CMMC requirements?

GCC High was created to meet the needs of DoD and Federal contractors that needed to meet the stringent cybersecurity and compliance requirements of NIST 800-171, FedRAMP High, and ITAR, or who need to manage CUI/CDI.

Q. Suitable for storage of CUI?

Yes.

Q. When updating your survey in SPRS, do you start a new one or can you edit the previous survey?

According to the guide here, one can edit their previous entry.

Q. Is it necessary to have an SSP for every system and operation or can an overarching SSP be used? We have several ways that we operate, depending on customer needs.

The answer is that it depends. Similar or connected systems can be covered by the same SSP as long as you clearly show the demarcation of those systems. However, stand-alone systems or those that require different operation models would need their own SSP.

Q. Would be interested in how the DAM Basic Assessment report can be generated for SPRS submission?

Exostar has tools that help generate your SPRS scores and how you are doing for CMMC/NIST compliance and to assist you in creation of your policies. For the DAM Basic Assessment report, you can utilize our Certification Assistant product including a free trial, information and sign up for that trial are located here.

Q. Hello, I am just starting to learn this information for my company. It feels like information overload. How can I keep my head above water to execute the protections to cover my company?

You may want to take a look at two of our other solutions Certification Assistant and PolicyPro. These can help you get started with your compliance journey and each of these have a free trial so you can see if they fit your needs.

Q. As a subcontractor, how will we know if a part is CUI, will CUI be clearly noted on the purchase order?

This will be a discussion you will need to have with the prime contractor(s) you are working with, and what do they consider CUI. You will need to provide to them the assertions are necessary to fulfill the contract requirements.

Q. Is the DoDAM excel template or similar available in our existing Exostar account somewhere?

You may want to take a look at two of our other solutions Certification Assistant and PolicyPro. These can help you get started with your compliance journey and each of these have a free trial so you can see if they fit your needs.

Q. Expert advice on GRC and CMMC, recommended tools, approach?

You may want to take a look at two of our other solutions Certification Assistant and PolicyPro. These can help you get started with your compliance journey and each of these have a free trial so you can see if they fit your needs.

Q. We are a European subcontractor of major US DoD contractors designing/manufacturing subsystems. Which CUI categories would be applicable to subcontractors like us?

CUI is itself a classification of data, "Controlled Unclassified Data" specifically, the agreements you have with your customers should inform you on what is necessary in the fulfillment of those agreements.

Q. Is Office 365 GCC required for all employees in order to qualify for CMMC?

No, this is one method to assist you in reaching your CMMC Level goals and depending on which level you want to achieve, the information, policies, users, etc. will depend on the approach and tools you want to use.

Q. I understand there are only 2 companies certified to audit. Do you know why this is? The Gov't expects everyone to be certified (audited), yet there are not near enough companies certified to do the work.

There are a number of audits/certifications/requirements etc. that are necessary to contract with and across Highly Regulated Industries. These requirements and audits do change as well and there is a lag from the market to catch up with the latest needs. I'm not sure which audit you are referring to, so I do not know the number of companies that are certified to conduct an audit.

Q. What Exostar is doing to make sure the data links it supplies are CMMC secure?

Exostar solve a number of issues with regard to data security and the links to that data. First and foremost, in our secure/federated/audited identity and access provisioning that is part of our Exostar Platform. This goes hand in hand with our Onboarding Module so our customers can provide additional safeguards with the organizations they choose to collaborate with. Lastly, we select Application Modules, in this particular case Microsoft 365 that can be hosted in the necessary environments to safeguard the data.

Q. Do I need an SSP ahead of time or will that be part of your company's responsibilities to customers who need the development aid?

SSP's are not one-time procedures documents so they should evolve as you change and adapt your tools, processes, and policies to fit your needs. Exostar provides additional products Certification Assistant and PolicyPro. These can help you get started with your compliance journey and each of these have a free trial so you can see if they fit your needs.

Q. Would this be an acceptable alternative to the full application access for long-tail suppliers with only a few documents a year?

Yes, this solution is a good fit for companies that do not require a full Microsoft 365 tenant of their own and all the capabilities that come along with that.

Q. Since we already use Microsoft 365 will we have to move to a different tenant?

No, you can continue to use your current tenant for your internal collaboration needs and utilize Exostar's Secure Access for Microsoft 365 to work with your partners and third parties.

Q. My company has multiple CAGE codes, for different manufacturing buildings within our campus which is all maintained within the same enclave. Do I need to register all my CAGE codes for SPRS or can I use just the CAGE code associated with our HQ which is where IT services are located?

You may want to check the various online training materials available for SPRS reporting. One resource is the User Guide available here.

Q. Will the new system be secure to the new CMMC cyber security requirements for encrypted file transfer of CUI data?

Yes, this solution will encrypt data during transmission.

Q. Does CMMC require our email and files be on MS365 GCC?

No, it does not require a particular tool or vendor, however utilizing Microsoft 365 hosted from GCC or GCC High may assist you in your CMMC requirements.

Q. I am in sales and want this cybersecurity requirement to be with my IT department, how do i make that happen?

You would need to discuss this with your organization.

Q. Would love to see a good example of a policy document for one of the families. Where would I find?

You may want to take a look at two of our other solutions Certification Assistant and PolicyPro. These can help you get started with your compliance journey and each of these have a free trial so you can see if they fit your needs.

Q. I have a real hot question for you. We are receiving multiple risk assessment questionnaires that ask to list in detail our deficiencies and to list practices we have implanted to address certain risk or controls of the 800-171/CMMC. Should we be sharing this sensitive information with them? I thought that was what the SPRS was for? My fear is that we need to send out redundant and more importantly extremely

sensitive information to all that ask. If this information was somehow intercepted or found out it could be used by an attacker and give them some attack vectors"

You should consult with your organizations Security Office or Legal Teams to determine what can be shared with outside organizations.

Q. As I just signed up with Exostar, general navigation and accessing supplier score cards are my first focus. Where should I look?

Please visit our Support Portal here, if you need training or information on our products.

Q. When is the deadline to become CMMC certified?

It has not yet been announced.

Q. Are there reports or logs what will support compliance to the standards?

Reports and logs become part of your material to auditors to prove that the policies and procedures you have in place are working.

Q. Does this replace what we already are using with ForumPass?

It may if you have the need for more real time collaboration with you partners that you get with Microsoft Teams.

Q. What's the best tool for complying at Level 3?

You may want to take a look at two of our other solutions Certification Assistant and PolicyPro These can help you get started with your compliance journey and each of these have a free trial so you can see if they fit your needs.

Q. Cybersecurity is a critical concern for all. However, I am a distributor. I sell pre-manufactured goods. Only invoices are stored on our system. No drawings, no sensitive information. Why must I meet system requirements equal to a manufacturer? Risk levels for suppliers of pre-manufactured goods require evaluation accordingly.

This will depend on the agreements and contracts you sign with your customers and partners.

Q. How do we get access to our POs?

It will depend on which Exostar customer you are working with. Exostar support pages should help you get started; those are located here.

Q. Potentiality to require defense industrial base based in allies' countries to comply with CMMC?

The potential exists. If you'd like to learn more Exostar hosts a number of CMMC Webinars. Links to our upcoming webinars can be found here; if you'd like to check out previous webinars, those recordings can be found here.

Q. Who do I need to speak to in order to learn how to navigate Boeing system for PO etc.?

We have help for the Boeing Portal available here.

Q. Exactly what is the difference between Certification Assistant & PolicyPro, & do we really need to subscribe to both? I understand they are both optional tools to help get the job done.

"These are companion applications that work together to help take weeks off the assessment process for NIST 800-171 compliance and/or CMMC.

Certification Assistant delivers a self-guided, step-by-step platform for streamlining the implementation of controls and policies necessary to complete an accurate NIST 800-171 self-assessment, or to prepare for CMMC success. Certification Assistant enables suppliers to understand each control, and the tools, processes, and policies needed to satisfy them in order to achieve full compliance. Moreover, because CMMC Level 3 is built on NIST 800-171, Certification Assistant provides a bridge to prepare for CMMC Level 3 certification.

PolicyPro saves you time and resources as you build and revise security policies in line with NIST 800-171 and CMMC directives. PolicyPro is an easy-to-use platform that helps suppliers create and customize policies to meet all 14 control family requirements within the NIST standard and 17 for CMMC. Once your policies are in place, use PolicyPro's assessment function to measure your compliance. It will evaluate and score your policy documents against model documents, taxonomies, and algorithms and generates a list of missing key words for gap assessment."

Q. When an organization implements MS GCCH, MS attests that the organizations meet the NIST 800 171 requirements, but I hear different opinions. What's not covered by GCCH?

Microsoft documents what groups should consider to move to GCC High here, including the requirements for those organizations that want to utilize here.

Q. Admin claimed MFA (or 2 factor) is in use because the laptop itself has a token saying it's allowed on the network and the user had to use a PIN or a password to log into the laptop. Is this truly considered MFA? Can the PC/Laptop be considered something you have? Also, my laptop will ask me for my PIN every time after it locks but I have not entered my password since setting up my laptop for work over 4 months ago. Would this not be a ding to an auditor for CMMC? Can you clarify exactly what will be looked at for 2FA or MFA?

Organizations make decisions on what their policies and procedures are and if they meet the needs for compliance. An audit by an outside agency will check to see if policies and procedures are followed and if they meet the necessary standard. You may want to contact an Exostar Partner that provides these kinds of services to assist the organization if you think there is a problem. Our partners can be found here, and click on CMMC.

Q. How does C3PAO conduct assessment of CMMC in Japan?

You would need to discuss this with the organization or individual that you have contracted with for the assessment.

Q. Is the prime contractor responsible for validating the subcontractors have submitted as score into SPRS and know if the score is of an acceptable rating? Also, do I have to submit an SPRS score if my organization handles ITAR, but does not have any of the applicable DFARS clauses (7012, 19, 20, 21)?

Organizations are responsible for their own scores, and your organization will be responsible for determining if your contracts require your SPRS scores to be submitted.

Q. How do you identify what is CUI within your environment?

There is quite a bit of training available for CUI material. One good source is the National Archives with training available here.

Q. Will you be providing a system for secure email with attachments including CUI (controlled unclassified information) and if so, will that system be CMMC compliant and at what cost?

No, this is not something that Exostar provides.

Q. As a software development company for Logistic support to a DOD Contractor MP.3.122 Mark media with necessary CUI markings and distribution limitations. is a challenge. Do we need to tag all our CTI (Design/analysis/etc. documents? All our developed screens in our application?

This is not an area that we are familiar with so would not be able to advise you, you may want to check with one of our partners that do provide services around compliance. A list of our partners can be found here, then click on CMMC.

Q. I would like to know about the latest schedule of C3PAO program roll-out to allied countries, namely Japan?

That question would best be answered by the CMMC Accreditation Body.

Q. How does this compare to 365 GCC?

This solution can utilize GCC High for the managed tenant.

Q. How can I find out what information that flows down to us is considered CUI? I've looked at the registry online but could use some clarification.

That is a question better answered by one of our service partners. A list of our partners can be found here, then click on CMMC

Q. Do you have any advice or suggestions on the scoping guidance and what to expect for scoping? What about whether the MSP and/or MSSP will be required to get CMMC compliant?

That is a question better answered by one of our service partners. A list of our partners can be found here, then click on CMMC

Q. Is all of this really needed for a small company that only supplies Vacuum Systems for Manufacturing Facilities? We don't ever see blueprints of layouts nor operational schematics; we just supply the fittings and Machines to clean up.

That will depend on your contracts with either a U.S. Government Agency or a Prime Contractor that has an agreement with you to satisfy a contract.

Q. When will 7012 apply to Non-DoD contracts? For RFP/RFI responses to DoD Contracts, do small businesses need to mention that they are in the process and/or exploring getting certified?

I have not yet heard of any guidance on this question.

Q. If a supplier has no contact with CUI is there still a NIST / CMMC compliance requirement?

NIST/CMMC does not only have to do with CUI, it has to do with policies and procedures that you have in place across all your systems. If you have a contract or agreement in place that have these requirements than you will need to comply.

Q. Are there any AI standards? Ex.: NIST

Artificial Intelligence (AI) is another system and is covered by CMMC and NIST. One of the key considerations with AI is the amount of data that can be generated.

Q. Have you heard about the recent changes Microsoft has made that don't allow users to designate safe senders when Microsoft has deemed the sender's domain to be potential phishing scams?

I have not heard of this and would be better addressed by Microsoft.

Q. Do the drawings we receive from our customer need to be marked CUI? They are telling us to consider everything they send to be CUI, even if they are not marked. Some drawings are marked for public dissemination.

If you are told that something is CUI, then it should be treated as such.

Q. Does this affect the usage for all the customers i.e., Boeing, Lockheed, Northrop Grumman, Bell Helicopter?

Secure Access for Microsoft 365 is a new product from Exostar, it will only affect those customers that subscribe to the product and those partners that they engage with through this offering.

Q. In looking into the process of self-assessment, it seems overwhelming to find even where to start. There seem to be no end of sites with vendors willing to contract with us. But there must be ways of handling this using our internal skill set along with our I.t. vendor to comply with the standards. So, the question becomes: is there an easy and streamlined way to proceed and make sure we are doing all we need to do in order to be compliant with CMMC and the NIST 800-171 standard?

You may want to take a look at Exostar's two products that help with CMMC and NIST 800-171 Compliance. They are Certification Assistant and PolicyPro.

Q. Regarding an Ethernet Private Line between two buildings, the provider says it does not need a firewall / encryption on the segment because it's "Layer 2 / EPL". I am concerned this constitutes a boundary and should have a firewall / encrypted tunnel between these two buildings, despite being an "ethernet private line". Can you speak to this to clarify the boundary and requirement to encrypt or not in this situation?

Sorry, but we are unable to address this particular question you may want to speak with one of our partners. A list of our partners can be found here, then click on CMMC.

Q. NIST 800-171 cross-over?

You may want to take a look at Exostar's two products that help with CMMC and NIST 800-171 Compliance. They are Certification Assistant and PolicyPro.

Q. We don't handle any classified information, will we still need to proceed with additional controls for information that we will never be viewing?

Your organization will need to determine the contracts and agreements that you have in place and what requirements and regulations to which you need to comply.

Q. Can you explain what a correct input is for the SPIRs website?

The user guide for SPRS is available here. You also may want to take a look at Exostar's two products that help with CMMC and NIST 800-171 Compliance. They are Certification Assistant and PolicyPro.

Q. Say I have only 3 users out of the 35 employees who ever have access to CUI. Do I have to lock down the entire organization or can I fence those 3 people off and apply the controls to them? For example, put them in their own VLan and contain them? While we certainly will be working on organization security, the solutions would look different for 3 vs the entire company.

You only need to secure CUI data and those users in your organization that should have access to it.

Q. Why is this system so difficult to use our PI refuse to log into it as it wastes their time?

Please provide your feedback on our product to Exostar support here. We appreciate you letting us know the issues you are having so we can assist you and improve our product.

Q. We did business in 2019 using the Exostar MAG site, under our former company name, which has since been dissolved and we are a new company name. How do we get Exostar to recognize our new name, DUNS and Cage code? An email to me would be helpful, if this is too specific for the training. We have been using Microsoft 365 secure access since 2018.

Please contact Exostar Support here to assist with this question.

Q. How does the 'non-gov' version of Microsoft 365 prove CMMC/NIST/DFARS compliance?

CMMC/NIST/DFARS compliance will be shown by an organizations policies and procedures that address the various Sections/Focus Areas/ etc. that make up these rules and regulations. Organizations will be audited to prove that compliance. Microsoft 365 and the various zones in which it is available can be part of a company's strategies to help them address particular needs.

Q. We are the only Saudi Arabian shooting range manufacture GAMI approved in KSA, we have been chosen by Raytheon and are registered as one of their ESD, do we have to be NIST 800-171 compliant? Although we haven't gone into any business yet with Raytheon.

This will depend on your agreement with Raytheon and would best be addressed directly with them.