



# Effective Use of Enclaves to Reduce CMMC Scope

presented by Glenda R. Snodgrass ([grs@theneteffect.com](mailto:grs@theneteffect.com))

---

Creating enclaves to reduce the scope of a restricted environment is a time-honored approach to minimizing an organization's compliance burden. Some types of data readily lend themselves to this approach (e.g., credit card data, which is typically accessed only at the point of sale), while other types of data don't fit into this model quite so well.

In our work with contractors and suppliers for the U.S. Department of Defense over the past few years, we have seen many examples of both successful and not-so-successful enclaves. While the configuration of an enclave will vary widely from one organization to another, depending on factors such as industry, size, and organizational culture, there are similarities in the challenges that must be faced.

## Managing Access

The first challenge is to identify who actually needs access to this protected data. Most organizations start this process by drilling down to the operations side of the business. Obviously the engineers, the researchers, the people who make the widgets from the diagrams -- they need the access.

But is that all?

Think about what other functions in your organization might need access to contract data. Here are a few that come to mind:

- business development





# Effective Use of Enclaves to Reduce CMMC Scope

presented by Glenda R. Snodgrass ([grs@theneteffect.com](mailto:grs@theneteffect.com))

---

- contracts management
- legal/compliance
- accounting/finance
- security (physical & IT)

Any enclave created to hold protected data must be accessible to *everyone* who needs access to that data, not just Operations.

## Managing Information Exchange

The second challenge is getting protected information into and out of the enclave. To tackle this challenge, you need a clear understanding of your organization's data flows:

- How do you receive data?
- In what format?
- Via what means?
- Who in your organization receives it?
- Where do they store it?
- Who has access to it there?
- Who is it shared with (across your organization or outside it)?





# Effective Use of Enclaves to Reduce CMMC Scope

presented by Glenda R. Snodgrass ([grs@theneteffect.com](mailto:grs@theneteffect.com))

---

- What do they do with it?
- Where is it backed up?

Now think about how the current data flow can be restricted to an enclave. Consider how to restrict the exchange of data both internally and externally.

## Managing Processes & Technologies

Too many organizations choose a technological solution for their enclave, then try to adjust their business processes to fit the technology. *This is backwards.* There are many different products, tools, services and solutions available on the market, and each fits differently into a given data flow. Understand your current business processes, map out the changes required to restrict access, then choose the technology that best fits your model.

The next decision is whether your enclave will provide only a means of storing and exchanging protected data, or also manipulating it. The tools required can be very different.

File Transfer. Some organizations set up a secure file transfer process to exchange data externally, creating a very small enclave outside the corporate network. Typically only a handful of users can move data from this enclave and to the internal network (or vice versa, move data there for a third party to retrieve). There may or may not be an internal enclave as well, depending on your data flow requirements.





# Effective Use of Enclaves to Reduce CMMC Scope

presented by Glenda R. Snodgrass ([grs@theneteffect.com](mailto:grs@theneteffect.com))

---

Email. If you set up an enclave that includes email, it will be a separate email address for each user in the enclave. Can your employees deal with having more than one email address? Can your customers?

If you set up an enclave that doesn't include email, you will either need a file transfer mechanism as discussed above, or a means of encrypting files locally before transmitting via some other path.

Both these paths require everyone to recognize FCI/CUI and possibly mark it prior to transmission. Do you have this capacity in-house? Do your current tools allow for this, or will you need to add tools to your environment (along with training on proper use).

Virtual Desktop Infrastructure. VDI is a popular method of creating enclaves. VDI has the advantage of creating an entire work environment, not merely a data storage and transfer tool. If you go this route, be sure to spec out the system to handle the tools your people need to use on the protected data -- engineering software, for example, can be resource-intensive and may not run on the operating system available in the VDI. Not all VDI solutions allow you to install software, or it may be an extra charge.

Isolated Network. Some organizations stand up an isolated network, with no connections to other networks nor the Internet, for protected data. This scenario works only in very limited circumstances, where protected data will be created on the isolated network and stay there, or be shared only via narrow options (encrypted external drive, burned to disc). This approach also creates





# Effective Use of Enclaves to Reduce CMMC Scope

presented by Glenda R. Snodgrass ([grs@theneteffect.com](mailto:grs@theneteffect.com))

---

compliance challenges, as some standard security requirements are difficult or even impossible to implement on an isolated network, requiring compensating controls, enduring exceptions or waivers. (For example, AU.L2-3.3.7 – AUTHORITY TIME SOURCE *"Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records"* is difficult to do in an air-gapped environment.) Think carefully before following this path.

**Important Note: You will need well-defined processes and employee training to make any of these scenarios viable.**

## Managing Expectations

Finally, managing the expectations of your employees and third parties (customers, vendors, partners) may be the most challenging of all. What seems simple and reasonable to the IT department is often ... *not* seen that way by others in the organization. Some third parties may require that you use their enclave rather than your own. Some may balk at the technologies or the methods you have chosen. Some will simply do what they want no matter what.

The key to managing expectations is to be prepared. If you have properly mapped your data flows, understand existing business processes, choose the technological solution that most closely aligns with these three critical elements, *and* provide employee training on proper (rational, functional, doable) procedures (as well as how to deal with the inevitable spillages), your enclave can be a success.

