NSA Policies:
A Guide for Mitigated Companies

"Policies" usually refer to some binders on a shelf that may be consulted when something unusual happens. Policies mandated by National Security Agreements (NSAs) are different. They must be executed continuously, and as written, or the mitigated company could be found to be in breach, which can be very costly indeed.

An NSA may require a number of policies, plans, and procedures (henceforth simply "policies"), dealing with Cybersecurity, Visitation Control, Technology Control, Personnel Security, Electronic Communications, and so on. The mitigated company is responsible for providing draft policies to the CFIUS Monitoring Agencies (CMAs) for review and eventual approval. Translating the NSA's requirements into *practical, executable* policies which are acceptable to CMAs is not only an art, it is perhaps the most important step in ensuring compliance and avoiding government sanctions.

Kaerus Consulting LLC has assisted with the drafting of many policies for mitigated company clients. This paper shares our experience and advice for drafting practical policies that ensure compliance with NSA requirements.

1. Communicate with Staff.

Early in the NSA negotiation process, consider an introductory all-hands meeting to introduce the CFIUS process and how it will impact the company. The main point of the meeting is to reassure the staff, which might have heard rumors about the government spying on them or might be worried that their jobs are at risk. Ignorance creates fear. Employees have confessed to us that they searched for "CFIUS" on the internet in an attempt to understand whether they might lose their jobs. Management transparency can dispel rumors and maintain morale.

Once they understand the process, operating staff should be asked to review draft NSA requirements before every turn during negotiations. The most common source of difficulties complying with a final NSA is the failure to consult the people who must implement the eventual

Agreement and who can tell you whether a particular term is feasible, feasible but costly, or infeasible.

2. Read and understand the final NSA.

Once an NSA is signed, it is important to step back and see the whole picture. We begin with an introductory read through of the entire NSA. Our focus during this first reading is to gain a general understanding of the overall document, its purpose, concerns, and the level of detail it demands. The CMAs will always state that every part of an NSA is equally important, but this is our chance to identify the provisions that require action. Often, critical impediments are buried in a seemingly-minor subsection within the document. Identifying these potential problems before starting to think about implementation saves a lot of time and effort.

Next, we read through the entire NSA line-by-line, stopping to list every concrete requirement. We refer to these requirements as specified tasks. Only tasks that are spelled out explicitly fall into this category, so they are easy to recognize and extract.

Once we have identified and documented the specified tasks, it is time to focus on the document's implied tasks. These are items that are necessary for the specified task to be achievable. For example, if the specified task is to deny access to certain people or organizations (which is a common restriction in NSAs), then an example of implied tasks inherent in that specified task might be:

1. Control access
2. Track access
3. Report access (in order to demonstrate compliance)
4. Contingencies (Fire alarms, evacuation, police response, etc.)

And so on. It is important to be as concrete and specific as possible with implied tasks. With a little thought, it is usually possible to specify each implied task with a single sentence or bullet point.

We then move on to the supporting systems. What software, hardware, infrastructure or equipment is required to support, demonstrate, and document compliance with the specified and implied tasks listed above? For example, a small facility, with very little traffic, may adequately

document access with a pencil and paper log. Larger facilities with more complex environments may need to utilize personnel badging, access fobs, ID checks, and Visitor Management Systems.

Once the list of specified tasks, implied tasks, and required supporting systems is complete, they should be organized into a matrix or flow chart showing dependencies. For example, automatic visitation logs require access systems which require smart badges or fobs.

3. Incorporate Operator Input.

Next, share the matrix or flow chart with the affected staff. Go over the task list by line item so all requirements are clear and ask for the staff's help. They will typically then take ownership of planning and the eventual implementation. Since they hold the tacit, institutional knowledge required to best solve practical problems, they really represent the shortest path to effective solutions and an executable plan. Better still, it's their plan. Once they own it, they are far more effective at getting it done.

First-line managers and operators may also be able to suggest an existing process or procedure that is close enough to what is envisioned by the NSA that it can be enhanced, modified, or copied to a large extent to meet an envisioned requirement. For example, existing safety and anti-shrinkage programs can be reframed for physical security. The more you can utilize existing work, the lower cost and more effective your program is likely to be.

First-line managers can provide the estimated time necessary for each item on the requirements flow chart, allowing the construction of a Gantt chart to guide the rest of the implementation process.

4. Draft Policy Documents.

The Gantt chart, combined with operating staff input, provides the raw material to draft policy documents. The drafting process, including CMA feedback, usually take months depending on the level of complexity, but some shortcuts can speed it up.

Boiler-plate items that introduce the project, property or business in general terms can often be sourced directly from existing company materials. We also use a general set of headings which can and should be modified, removed, or added to, to meet the specific requirements of the NSA. The most common are:

- Introduction
- Revision History
- Purpose
- Scope
- Exemptions
- Key systems
- Key Personnel
- Distribution Controls
- Disclosure Controls
- Physical Access Controls
- Electronic Access Controls
- Communication Security
- Training
- Whistle Blower Program

Forms, logs, distribution lists, acknowledgement forms, reporting matrices, access applications, badge requests, reports, personnel lists, rosters, other lists that change or will be updated periodically and other reusable documents should be included in appendices.

We find that drafting the purpose and scope sections is best left to the end, after the detailed sections of the document have been completed. Exemptions, exceptions, and alternate procedures are a good place to hold anything that is difficult to implement. These are generally the last section to be completed.

It is sometimes possible that some requirements of the NSA may be exempted for certain components of the business's operations, and the company will still achieve overall compliance with the NSA. These items should be discussed with CMAs to understand their flexibility. Most

of the time, a bit of creativity can resolve the concerns, but in some cases obstacles to implementation remain.

5. Address Obstacles with CMAs.

Significant obstacles to compliance with an NSA should be discussed with CMAs as soon as they are identified. Forthrightness and timeliness go a long way in establishing a positive relationship with CMAs and in encouraging CMAs' willingness to be flexible. CMAs may be willing to postpone certain provisions in the NSA or to not invoke a provision at all (such as the requirement to engage a Third- Party Auditor).

In our experience, it is also important to provide one or more potential solutions for each obstacle reported to CMAs. Generally, CMAs will be open to discussing compromises as long as the proposed solutions protect National Security as much as the original framework. Outside counsel may be able to help because of its familiarity with the original negotiations and understanding of what the government is trying to accomplish.

Ultimately, the NSA is a legally-binding contract, and the transaction parties are obligated to comply with it or face monetary penalties up to the size of the transaction and/or a complete divestment order.

6. Finalizing the Documents.

Numerical sections and subsections provide a concrete reference points which are useful in discussions and correspondence. We utilize something like the following:

1: Section Heading (e.g. Training, Key Personnel, etc.)
- 1.1: Subsection X (Usually a specified task)
  - 1.1.1 Subsection 1 of X, (Usually an implied task)
  - 1.1.2 Subsection 2 of X
- 1.2 Subsection Y (Usually another specified task).
- 1.3 Subsection Z

Once the document is organized, give the staff time to review it and provide feedback. If everyone has been involved up to this point, there should be few questions or concerns. Remedy anything requiring clarification or changes and submit the draft to the CMAs for review. Generally, most CMAs will have some questions and some preferences as to how things may be reported, executed on the ground, or drafted into the document. Once those are addressed, you can finalize the draft and submit for acceptance.

Contact: Albert Schultz, 571-243-2492, albert@kaerusllc.com