DoD Office of General Counsel

Legal Discussion: Policies and Practices Regarding Monitoring and Consent

DIB Cybersecurity Pilot Meetings
December 09, 2011

(b) (6)
Associate General Counsel
DoD Office of the General Counsel

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Disclaimer

- This briefing is being provided for informational and discussion purposes only and does not constitute legal advice, nor create any attorney-client relationship. The Department of Defense Office of General Counsel is not acting as your attorney. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this briefing. We likewise do not warrant the legal effect of these materials.
- The law changes very rapidly and, accordingly, we do not guarantee the accuracy or currency of this information is accurate and up to date. The law differs from jurisdiction to jurisdiction, and is subject to interpretation of courts located in each state or county. Legal advice must be tailored to the specific circumstances of each case and the tools and information provided to you may not be an appropriate fit in your case.
- The opinions expressed in the presentation of these materials are those of the individual contributors to or presenters of these materials and do not necessarily represent, and should not be attributed to, the Department of Defense or the United States Government.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Agenda

9:00 – 9:15	Welcome and Introductions	DoD
9:15 – 9:35	Status Update and Path Forward on the DIB Pilot Evaluation and Extension	DoD, DHS
9:35 – 11:55	Legal Discussion: Policies and Practices Regarding Monitoring and Consent • Update/Lessons Learned by DIB Partners Regarding Assessment and Implementation of Consent Mechanisms (DIB Companies) • Feedback and Discussion of Pilot Legal Construct for Addressing Consent and Monitoring -- Recommendations for the Way Ahead (Open Discussion)	DoD, DHS, DoJ, DIB
11:55 – 12:00	Closing Comments and Next Steps	DoD, DHS

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

More Specifically

9:35 – 11:55	Legal Discussion: Policies and Practices Regarding Monitoring and Consent	DoD, DHS, DoJ, DIB
	• Update/Lessons Learned by DIB Partners Regarding Assessment and Implementation of Consent Mechanisms	DIB Companies
	• Feedback and Discussion of Pilot Legal Construct for Addressing Consent and Monitoring -- Recommendations for the Way Ahead	Open Discussion

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Please Keep in Mind...

1. The "Discussion Topics Regarding Monitoring & Consent Practices" is a SUGGESTED LIST of topics – to encourage and offer structure to an open discussion of complex issues . . . not intended to limit
2. Participation in the discussion or survey activities is absolutely 100% VOLUNTARY.
3. All of the discussions will be NON-ATTRIBUTIONAL.
4. Any written responses, or other documentary materials (*e.g.,* samples of updated banner language), will be ANONYMIZED – with several options for doing so

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Excerpt from the FA Amendment

Under SECTION X: GENERAL PROVISIONS, *Add the following*:

"1. The Parties will conduct their respective activities under this FA, including all amendments and attachments, in accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data. By signing FA Amendment #—

"1. The Government is confirming that it has performed a review of its policies and practices that support Government activities under this FA, and has determined that such policies, practices, and activities comply with applicable legal requirements; and

"2. The Company is confirming that it has performed a review of its policies and practices that support Company activities under this FA, and has determined that such policies, practices, and activities comply with applicable legal requirements, and include measures that the Company has determined are legally sufficient to ensure authorized user consent to the interception, monitoring, access, use, and disclosure of electronic communications or data residing on or transiting Company systems, including the disclosure of related information to the Government as provided in this FA."

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Discussion Topics

1. Was the pre-pilot guidance (*e.g.*, the 8 key elements for notice & consent banners) provided by the USG valuable in identifying or addressing these issues?

   a. Were there any elements of the guidance that were not clear, not applicable, or otherwise not helpful?

   b. Is there any additional information, or other forms of assistance, that might be more helpful?

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Discussion Topics

2. Has your company elected to revise or update its logon banners or other means by which it obtains user consent? (Or are you considering doing so now, or in the near future?)

   a. If so, were these updates facilitated by the guidance or discussion of these issues in connection with the pilot? What types of considerations drove these changes?

   b. What are the primary challenges, and the typical time frames required, in making changes to your company's logon banner or other mechanisms used to secure consent?

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Discussion Topics

3. As an update to the previous survey of notice & consent practices initiated in December 2010:

   a. What are the primary mechanism(s) your company uses to achieve user notice and consent (*e.g.,* log-on banners, user agreements, workplace policies, employee training).

   b. What is the operative language your company uses to obtain user consent for monitoring and disclosure of information (*e.g.,* copies of logon banners or user agreements, excerpts from company policies or employee training, description of other notice procedures).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Discussion Topics

4. Has your company experienced any unanticipated issues or significant challenges regarding implementation of its notice & consent mechanisms? If so, please describe them.

5. Some companies have indicated that they also rely significantly on legal theories other than notice & consent (*e.g.,* "rights and property") for some elements of their information security practices. What are the other legal theories or mechanisms (*i.e.,* other than notice & consent) that may apply to the types of monitoring or information sharing activities under with the DIB pilot? *Note: this question is not intended to elicit any specific, attorney-client privileged information -- only to identify applicable legal theories.*

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Discussion Topics

6. The DIB pilot activity utilized a certification approach regarding each company's individual determination of the legality of its policies and practices, including user notice & consent –

   a. Would this approach be effective in a permanent DIB program with expanded participation?

   b. Are there other approaches to addressing these legal issues that should be considered?

   c. Do you have any other recommendations or suggestions for addressing these issues in any future implementation of the DIB pilot or related information sharing activities?

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Discussion Topics

Did we miss anything?

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

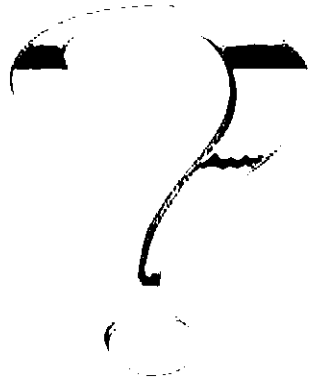
Questions?

(b) (6)

Associate General Counsel
Department of Defense
Office of the General Counsel

Direct: (b) (6)

(b) (6)



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

BACKUP SLIDES

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

DoD Office of General Counsel

Discussion Points: Key Elements for Notice and Consent Banners

Defense Industrial Base Cybersecurity
Exploratory Initiative Meetings
December 2-3 2010

(b) (6)
Associate General Counsel
Department of Defense
Office of the General Counsel

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Overview

8 Key Elements for Notice and Consent Banners

1. It expressly covers *monitoring* of data and communications *in transit* rather than just accessing data *at rest*.
2. It provides that information transiting or stored on the system may be *disclosed* for any purpose, including to the Government.
3. It states that monitoring will be *for any purpose*.
4. It states that monitoring may be done by the Company/Agency or *any person or entity authorized by Company/Agency*.
5. It explains to users that they have "*no [reasonable] expectation of privacy*" regarding communications or data transiting or stored on the system.
6. It clarifies that this consent covers *personal use* of the system (such as personal emails or websites, or use on breaks or after hours) as well as official or work-related use.
7. It is *definitive* about the fact of monitoring, rather than conditional or speculative.
8. It expressly *obtains consent* from the user and does not merely provide notification.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

1. **It expressly covers *monitoring* of data and communications *in transit* rather than just accessing data *at rest*.**

Notes:
- Use the terms "monitoring" and/or "intercept."
- This requirement is driven by the Wiretap Act and Stored Communications Act.

Examples:

- "You consent to the unrestricted monitoring, interception…of all communications and data transiting or stored on this system…."
- "You consent, without restriction, to all communications and data transiting or stored on this system being monitored, intercepted…"

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

2. **It provides that information transiting or stored on the system may be *disclosed* for any purpose, including to the Government.**

Notes:
- Both access and disclosure must be addressed in the banner.
- Unauthorized disclosure is a separate crime from unauthorized access under statute.

Example:

- "You consent, without restriction, to all communications and data transiting or stored on this system being monitored…or disclosed to any entity, including to the Government…"

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

3. **It states that monitoring will be *for any purpose.***

Examples:

- "…at any time and for any purpose…"
- "…at any time and for any purpose, including for cybersecurity purposes..."
- "…for any lawful purpose…"

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

4. **It states that monitoring may be done by the Company/Agency or *any person or entity authorized by Company/Agency.***

Examples:

- "…monitoring by or disclosure to any entity authorized by [Company]…"
- "…monitoring by or disclosure to any entity…at the sole discretion of [Company]."

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

5. It explains to users that they have "no [reasonable] expectation of privacy" regarding communications or data transiting or stored on the system.

Notes:

- This languages tracks the case law analyses at both federal level and many State laws
- Legally significant "buzz phrase".

Example:

- "You are acknowledging that you have no reasonable expectation of privacy regarding your use of this system..."

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

6. It clarifies that this consent covers *personal use* of the system (such as personal emails or websites, or use on breaks or after hours) as well as official or work-related use.

Notes:

- People may develop an expectation of privacy in their personal communications if they can access them from work. This needs to be explicitly addressed.

Example:

- "...including work-related use and personal use without exception..."

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

7. It is *definitive* about the fact of monitoring, rather than conditional or speculative.

Notes:

- If the language is too conditional with regard to monitoring, users begin to develop an expectation of privacy over time.
- In addition to definitive banner language, there should be no other representations that actual monitoring doesn't happen, or happens only seldom, in practice.

Example:

- "…will be monitored…" AVOID "may be" OR "reserves the right to"

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

8. It expressly *obtains consent* from the user and does not merely provide notification.

Notes:

- Click-through banners are best because they force the user to interact with the language.
- Supporting processes should also preserve/provide evidence of the user's agreement to the terms.

Examples:

- "By using this system, you are acknowledging and consenting to…"
- "By clicking [ACCEPT] below… you consent to…"

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

And the [almost] unspoken factor…

The rest of the banner …

(or associated policies, elements of user agreement, user training, etc.) …

must not be inconsistent with, or otherwise undercut, these elements.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~