NIST Framework Privacy Comments (Appendix B)

Asset Mgt: good that you call out knowing dataflow. But it's not just PII data, organizations should have a dictionary of types of privacy data, which is data that needs to be handled based on regulation or consent of owner. This could be healthcare data, PCI data, Financial Data (GLBA, OCC FFIEC, SEC, etc), or if multi-national organization that has European employees, EU privacy data, which is more than US considers PII.

Business Environment: There should be an understanding of the type of data required by HR, IT, IT Security, collected from customers or citizens, and what business process handles that data. In the US, there is no expectation of privacy on organizational network using organizational systems. But, in EU and some other countries, there is. There also needs to be a definition of the type data you will handle: data about your employees and customers (known as controller data), and data about your customer's customer (processor data), and how you collect it, online or offline. If personal mobile devices are in use, then larger privacy concerns exist, having personal devices under management could capture personal info, such as specific applications related to prescription drugs or medical condition monitoring, for instance.

Governance: extend regulatory requirements based on industry, region (state breach disclosure law, or international laws), and any personal requirements and consent of folks who give you data (if you collect any data as part of business). Privacy policies should be defined and posted on collection points (eg, web site, application, or mobile app). This is a good list for policies and procedures, but would add statement about transparency of these elements, and include one about Security, where once collected, data will be kept safe and secure from potential abuse, theft, or loss, with limited access control based on need to know.

Risk Assessment: this is a good addition about PII as a commodity. Holders must understanding not just regulatory risk to breach of privacy data, but there are black markets where some data has greater value than others (eg healthcare data most valuable now, Credit cards years ago, etc) to help prioritize protections. If mobile is in scope, and BYOD is used in some cases, consideration for privacy elements of that are important.

Risk Management Strategy: similar to above, a risk assessment of routine evaluations of what data is collected, what are the protection requirements, how is it collected, how long stored, etc. I can write some text if you want.

Access Control: current statements is more about system access, there needs to be call-out of human access based on need to know, and may be restricted by time or redaction of data as needed.

Awareness: no comments

Data Security: good point on lifecycle, but also includes all layers of manual and technical processing of data, from hardware, network, application, interface, physical storage, backup, etc.

Information protection: kind of redundant from data security. Maybe combine the two, the point about secure disposal is a good one.

Protective Technology: This is a good point to review the types of security protection and detection technologies to see what PII might be stored or used. Web and mail gateways, deep packet inspection, even configuration management products could be culprits. When we talk about mobile, and BYOD, this becomes very tough, especially for Mobile Device management and use of containers or virtualized environments to separate personal from organizational data.

Anomalies and Events: similar to point above, make sure you know what data detection technology accesses or stores. Even a web proxy might have some PII from user web interactions. Endpoint malware and DLP protections might also store or forward PII to back end systems, (or backed up) which could make it tough to identify all locations of protected data. I think last line about accuracy of PII data is not relevant to this section.

Security Continuous monitoring: good point to continuously review the data being collected, and where it might flow and be stored.

Detection Processes: excellent point! Privacy organization should be briefed on all current and future security detection and protection technology, and security procedures to consider privacy risks to the process.

Response Planning: I agree with the premise, but there is it's sometimes not known up front. A breach of a customer database or loss of laptop containing customer data is straightforward. But some internal miss-use, or recovery of a machine from malware infection might also reveal PII. I would bet in most incidents a responder has no idea what is PII. So, there should be a loop back to training of responders and forensics folks on PII identification and handling.

Communications: yes, there are 48 different state breach disclosure laws, many overlap or contradict each other. GLBA trumps them all for financial, HITECH now for healthcare. EU has even more stringent requirements. But another aspect is not just appropriate communications, but protection of data after an event. If there is a public filing due to regulatory audit, disclosure requirements, or in case of litigation, contents of the report that might become public might contain privacy data. Some organizations have the outside council contract the response vendor (if outsourced) to protect the report (through client privilege).

Analysis: ditto context from Response Planning. Responders need to be trained, the type of data protected is documented, and procedures to handle it defined.

Mitigation: I'd add the integrity of the data after mitigation is important, if yo restore data from backup, or repair or rebuild database, you want to ensure the privacy data is still correct and complete.

Improvements: this is repeat of Response planning. I think it's more simple, privacy training for all IT, security, response and forensics personnel. Socializing among the team the results of risk assessments, the expansion of the organization, data collection, customer or user base, regional coverage, etc, must be regular intervals.

Recovery Planning: I think this includes communications, disclosure, roles and processes etc. Again, making sure protected data was recovered, or any restoration is complete and accurate.

Improvements: Ditto Improvements from above.

Communications: Ditto from Communications above.