Times are a changing

The IT security landscape has been changing. Federal agencies are facing heightened pressure to rigorously protect data.

- Any data that passes through our hands
- From cradle to grave
- From theft, but also from intentional corruption

Federal agencies need to “certify” that data hasn’t been tampered with (data lifecycle documented and approved by an Information System Security Officer).
Why does SCAT care?

NOAA’s SCAT database

Now: on a single machine in the command post, 1 user
Future: on a server in the command post or on the web, many users

Government data can’t pass through or reside on a non-gov server

• Can’t use non-certified cloud services
• Data can’t pass through data collection servers
• Where do you securely archive SCAT data once a response is done?

Some specifics

• Non-gov servers must be FedRAMP certified: involves Assessment and Authorization (A&A) process
• Applications built on approved technology stacks (unix-CentOS, PostgreSQL, open source JavaScript libraries) get approved easier
• Accessibility requirements (section 508 compliance)
• Password standards (30 day expiration, no group accounts)
• Annual security scans
• Extensive documentation to validate IT Security standards have been met
Bottom line

Building SCAT software that’s usable by government agencies now take a lot more work than in the “old days”.

Headline

Text (flush left or centered)
Headline

Text (flush left or centered)