If it can be measured it can be improved

Andrew Artz

AFE Presentation | Friday 10. 2. 2020

Andrew Artz

Pathways Student (Computer Science)

Dual Degree Masters of Public Policy &
Masters of City and Regional Planning Candidate (May 2021)

Previously:

- Search & Extraction for CBRN task force
- Regional transportation committee
- Non-profit advocate for non-motorized transportation in mostly rural communities

Currently:

- Data wrangler and Splunk Power User
- Forecasting usage of the National Vulnerabilities Database
- Pitching new ideas to audiences with more experience *and* audiences with less technical backgrounds

If it can be measured it can be improved

Mission

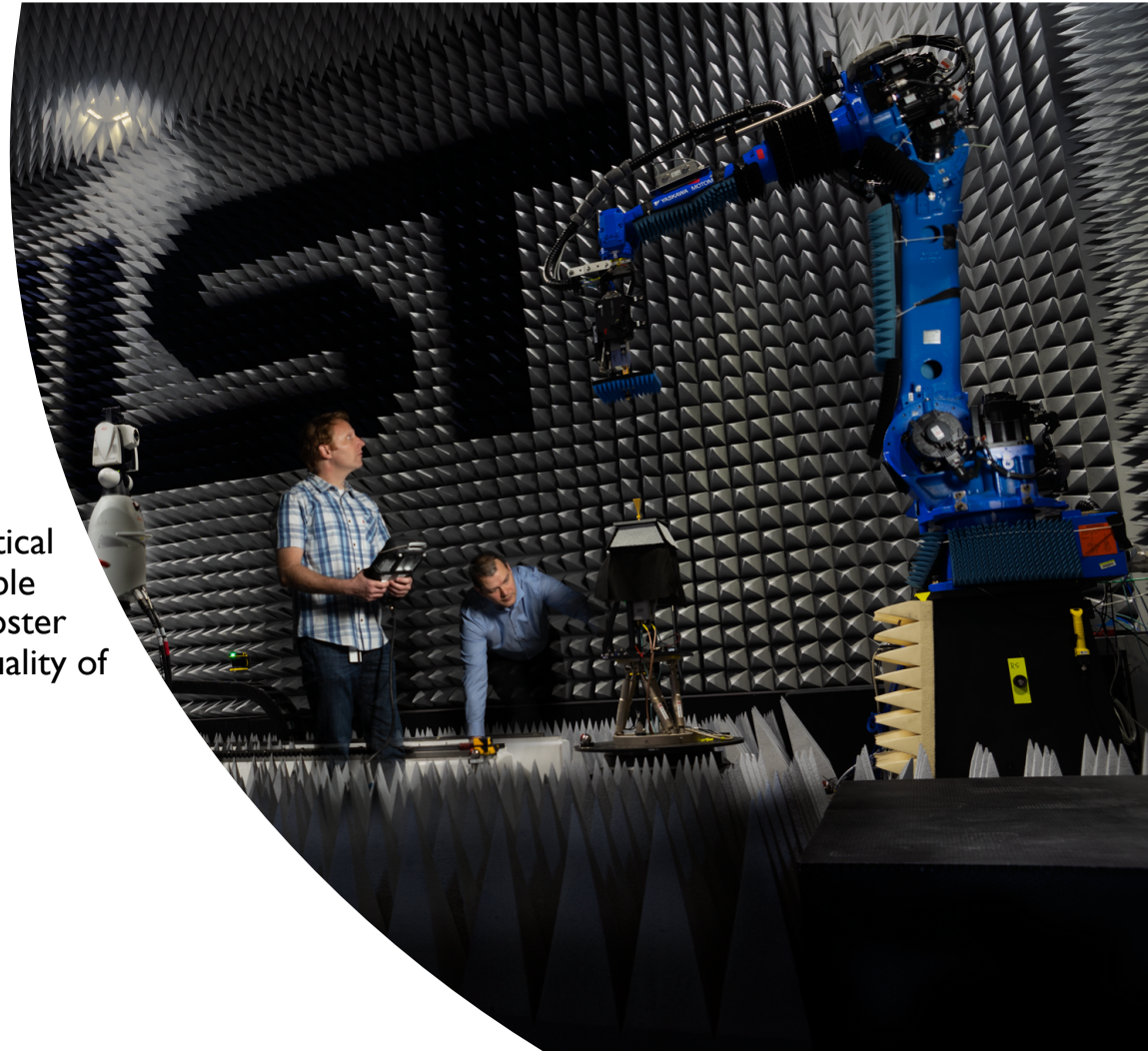
To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Vision

NIST will be the world's leader in creating critical measurement solutions and promoting equitable standards. Our efforts stimulate innovation, foster industrial competitiveness, and improve the quality of life.

Core Competencies

- Measurement science
- Rigorous traceability
- Development and use of standards



U.S. Department of Commerce

NIST

ITL

COMPUTER SECURITY DIVISION

SECURITY TESTING, VALIDATION AND MEASUREMENT

NVD

Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated March 27, 2020

Disrupted Federal Elections: Policy Issues for Congress

Introduction

The coronavirus disease 2019 (COVID-19) outbreak has renewed interest in how election administrators and political campaigns prepare for emergencies and natural disasters. Some states have postponed primary elections. Political campaigns have expanded online outreach in lieu of in-person events. According to media reports, national party conventions are proceeding as scheduled, but contingency plans are under consideration. Legislation has proposed additional funding and voting options in federal elections. As of this writing, legislation and elections planning are changing daily. This product will be updated periodically.

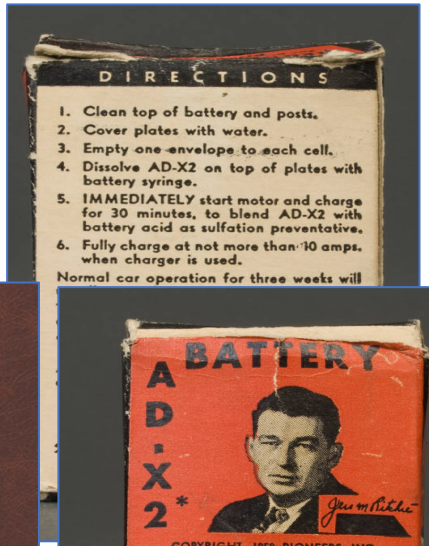
This updated CRS In Focus briefly introduces historical and policy issues that could be relevant for congressional oversight, legislation, or appropriations related to what this product calls *disrupted elections*. This term means events such as natural disasters, other emergencies, or cyberattacks that could substantially delay or prevent normal voting, election administration, or campaigning.

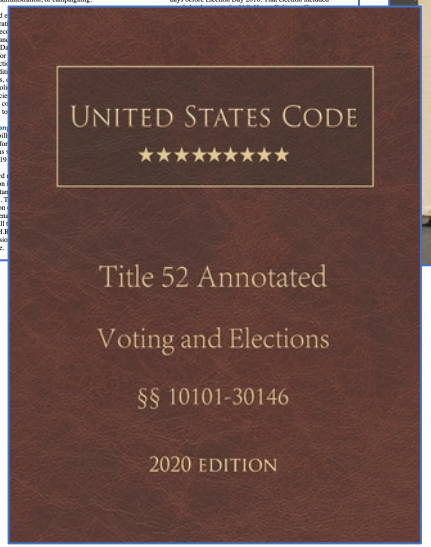
- S. 1397 would require states to accept a federal write-in ballot. Currently, the only such ballot is the Federal Write-In Absentee Ballot (FWAB), a backup federal ballot for military and overseas voters (discussed below) whose state ballots do not arrive on time.
- S. 3440 and H.R. 6202 would require states to establish voting contingency plans for, and require states to accept absentee ballots during, certain declared emergencies. S. 3529 contains similar contingency and absentee voting provisions, and would extend additional voting options and requirements to subsequent federal elections.

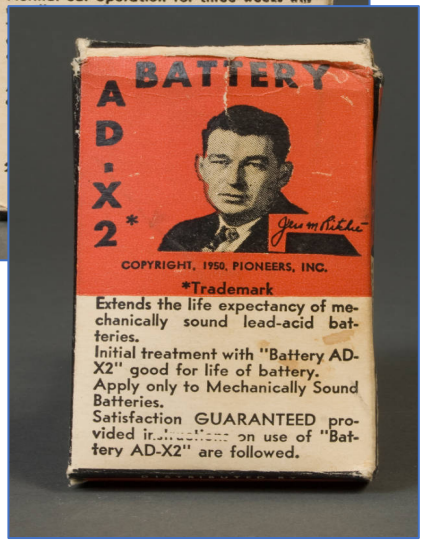
Selected Recent Examples

COVID-19 is a recent and prominent example of election disruption, but is by no means the only such example.

- Super Typhoon Yutu struck the Commonwealth of the Northern Mariana Islands (CNMI) approximately 10 days before Election Day 2018. That election included







CVE-2020-11500 Detail

Current Description

Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

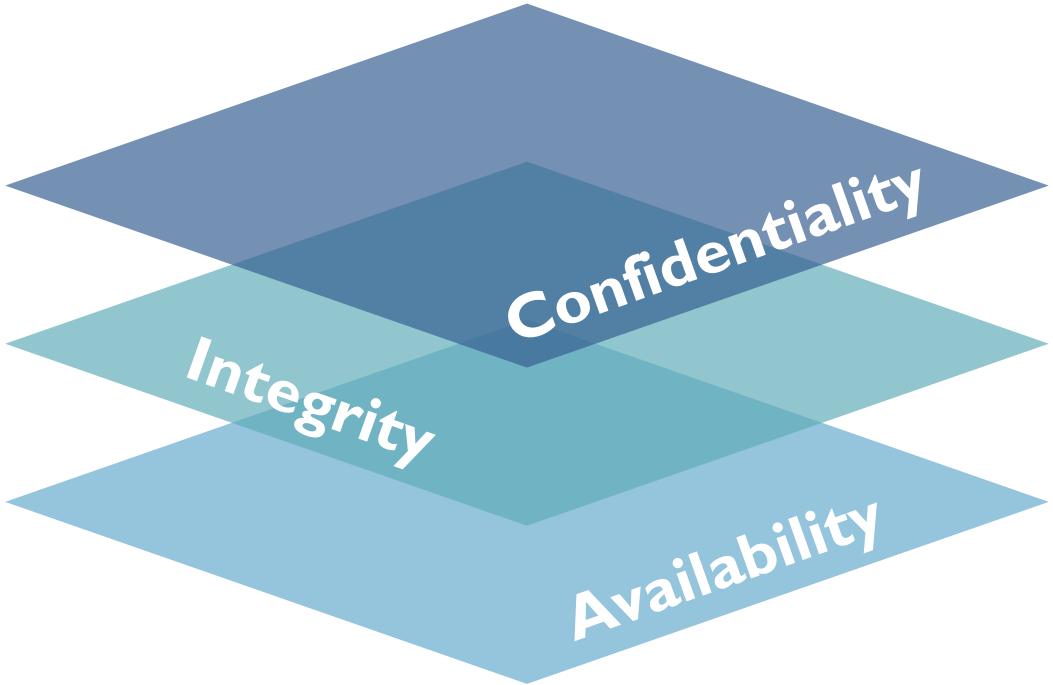
NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

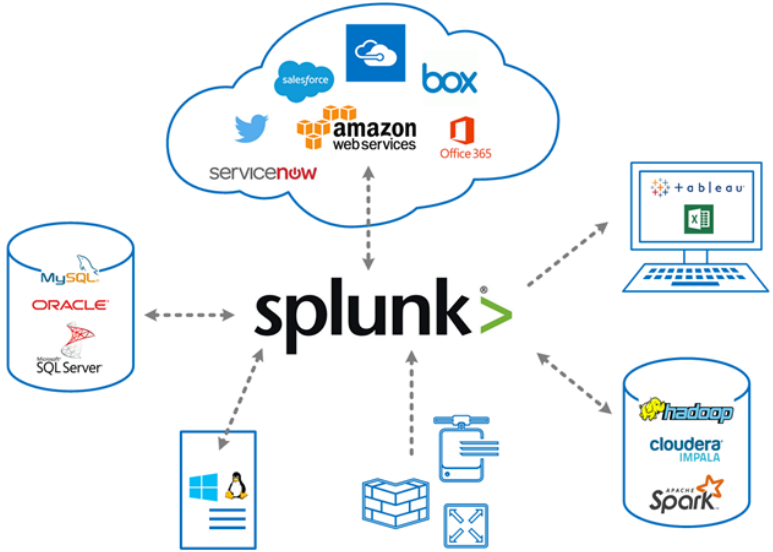
CVE Dictionary Entry:
CVE-2020-11500
NVD Published Date:
04/03/2020
NVD Last Modified:
04/07/2020
Source:
MITRE

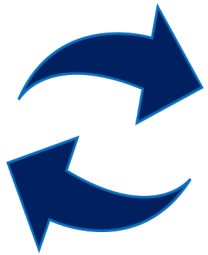
The Objectives of Information Security

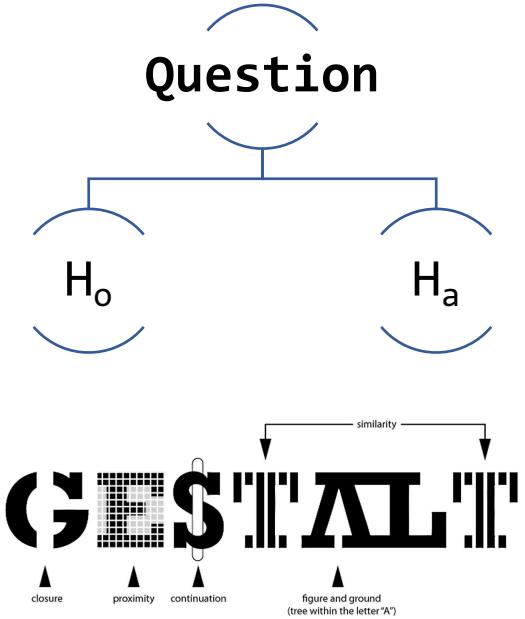


NIST Special Publication 800-12, revision 1 *An Introduction to Information Security* section 1.4

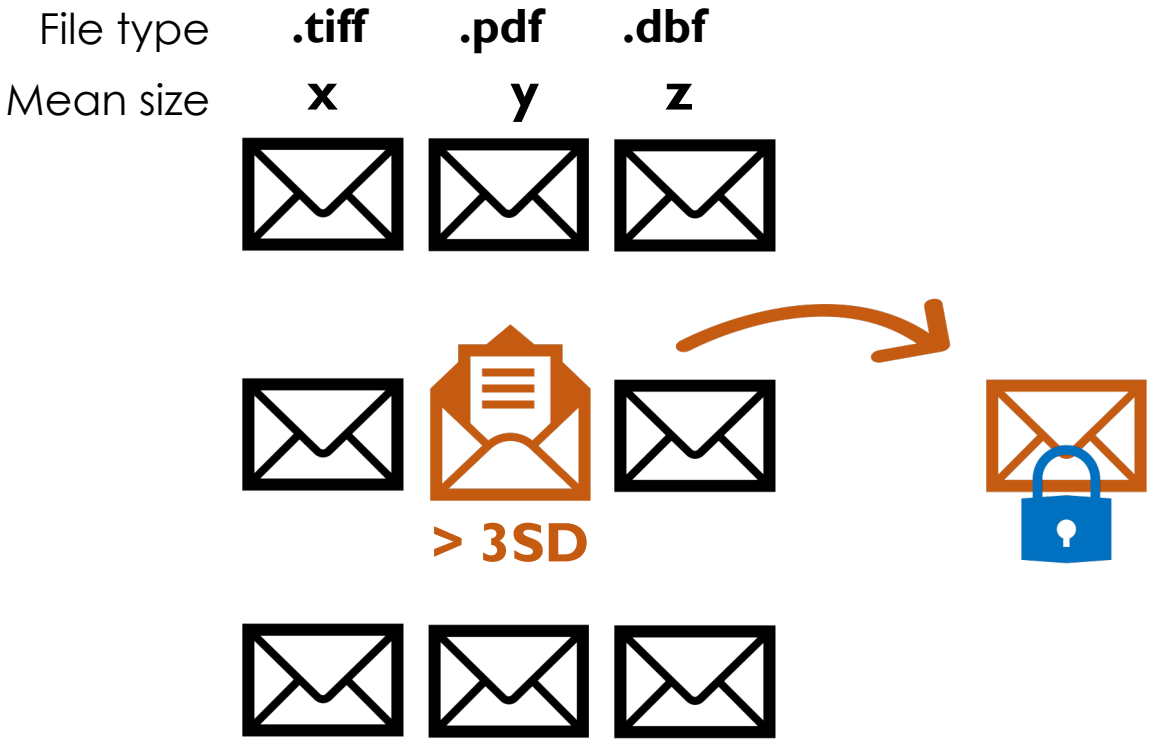
A “normal” day


salesforce
box
amazon web services
Office 365
servicenow
MySQL
ORACLE
Microsoft SQL Server
splunk>
+ableau
hadoop
cloudera IMPALA
Apache Spark




Question
H_o
H_a
similarity
closure
proximity
continuation
figure and ground
(tree within the letter "A")

Example: Lock suspected ransomware



When one door closes

My major takeaway: Triage

My old model:

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

My new model: $[SPV = R]$, or Severity *Probability *Value = Risk