California ISO

DMARC Adoption @ RC West

Hubert Hafner
Senior Advisor, Information Security, California ISO

November 2022

Agenda

- What is DMARC ?
- DMARC Adoption world wide
- DMARC Adoption @ US government entities
- Differences in DMARC policy, the Value of Initial DMARC Policy p=none
- Example DMARC Policy Transition Timeline and Impact (caiso.com)
- DMARC Adoption @ RC West, Call for Action
- Summary & Next steps

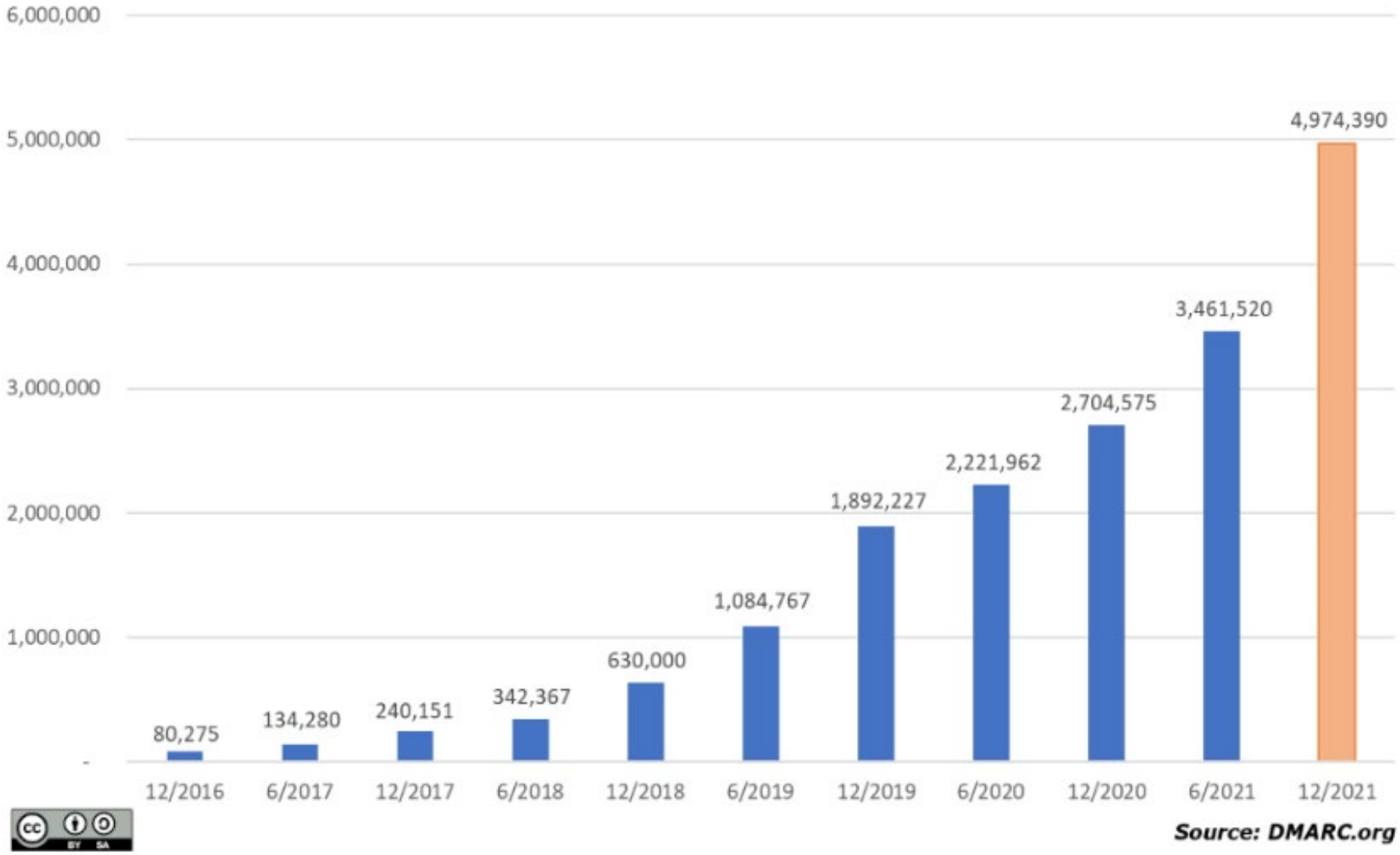
- Additional information in back-up slides
  - Implementing DMARC Best Practices

What is DMARC ?

- DMARC = **D**omain-based **M**essage **A**uthentication, **R**eporting & **C**onformance
- DMARC, first announced in January 2012, is considered the industry standard for email authentication to prevent phishing email attacks in which malicious third parties send harmful email using a counterfeit address.
- By implementing DMARC, companies lower the odds of their domains being spoofed and used for phishing attacks.
- In 2017 Department of Homeland Security's (DHS) issued binding operational order to all government agencies to implement DMARC
- By the end of 2019, 30.3% of 21,075 domains analyzed had a DMARC policy in place. Since then adoption rate of DMARC has steadily increased
- DMARC is listed as one of the 153 safeguards of Center of Internet Security (CIS) Critical Security Controls® (CIS Controls®) v8, Implementation Group 2

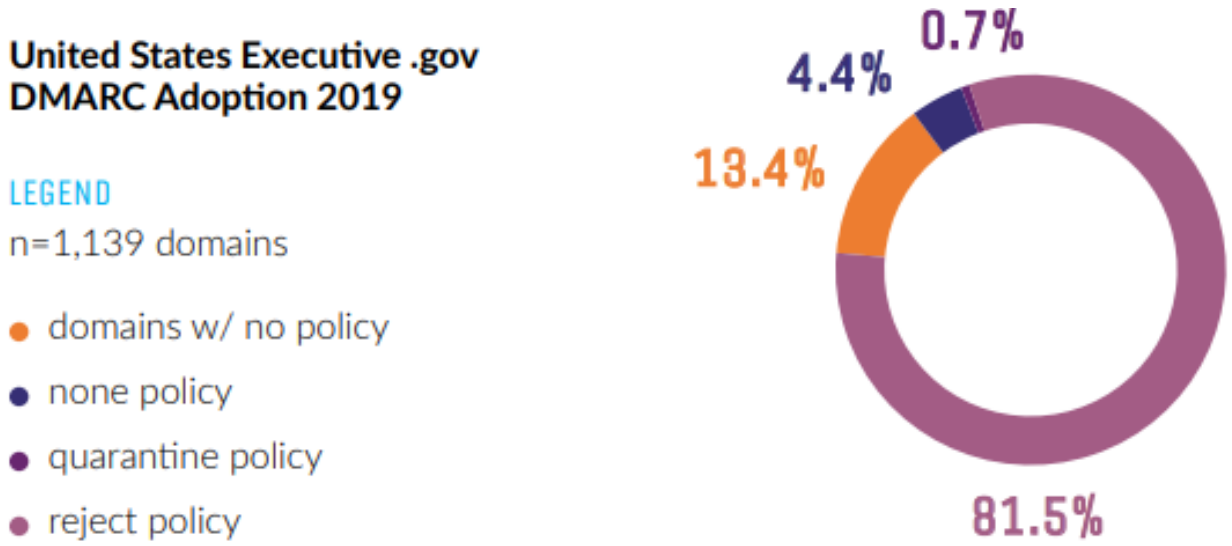
Sources: DMARC.org; 250ok's Global DMARC Adoption 2019 report, https://www.helpnetsecurity.com/2019/07/17/companies-dmarc-adoption/

Trend of Valid DMARC Records Confirmed via DNS



DMARC Adoption @ US Executive Branch

- In October 2017, the Department of Homeland Security's (DHS) issued binding operational order 18-01 requiring the executive branch of the government to move to a reject policy.
- By 2019, 86,4% of 1,139 sampled domains had a form of policy in place.



- As of 2022 all government entities are required (and expected) to have reject policy implemented.

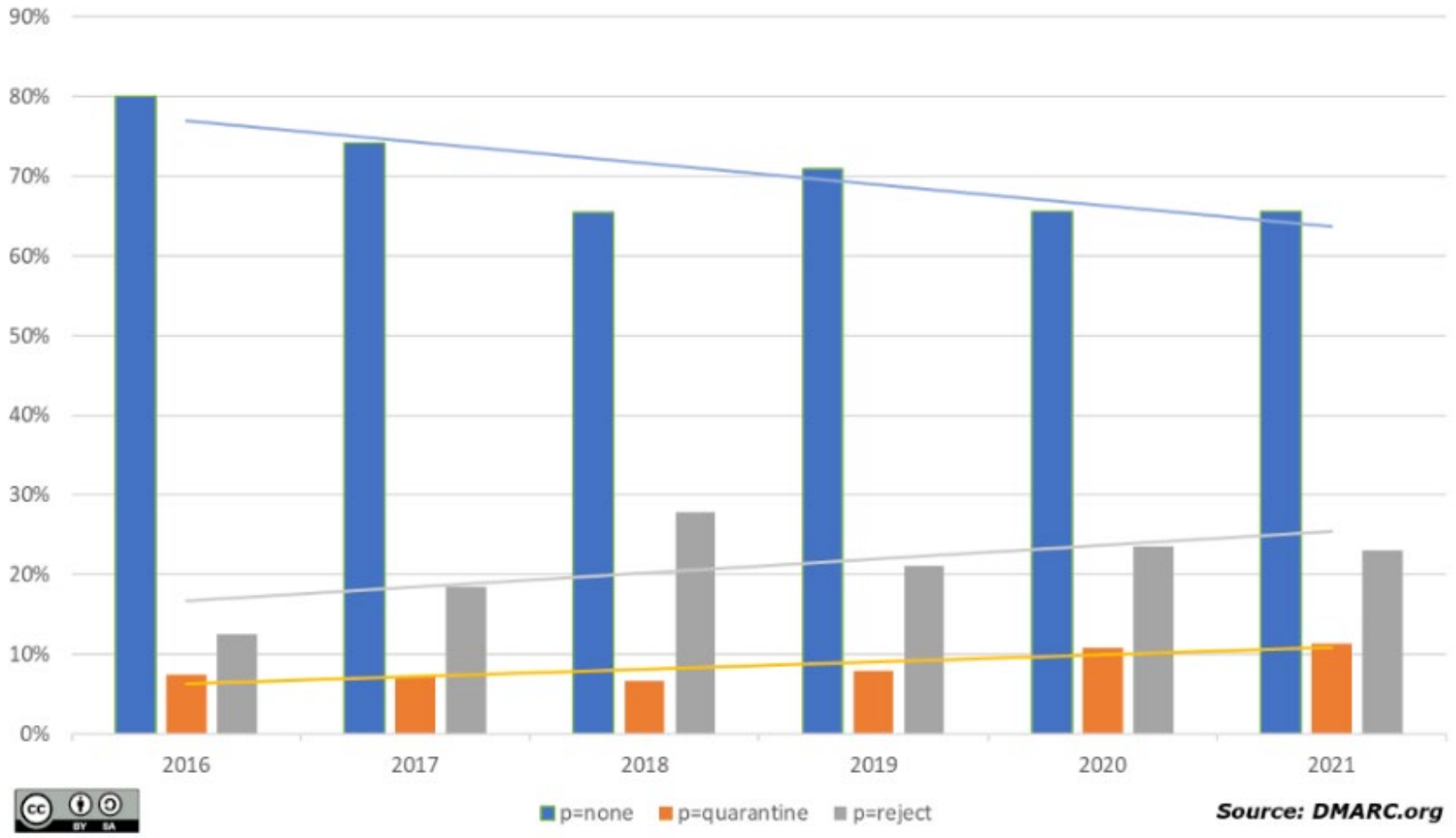
Differences in DMARC policy

- No policy: no DMARC entries in DNS of domain owners.
- **p=none**: no action requested by domain owner when DMARC verifications fail
  - Start of DMARC implementation indicating initial DMARC DNS records have been configured and the domain owner is fine tuning all his email sources.
  - It may take several months or years to get all email sources configured, e.g. for email sent by service provides on behalf of domain owner.
- **p=quarantine**: DNS owner asks you to quarantine all emails that fail DMARC verifications. Sender of email receives no rejection notice.
- **p=reject**: DNS owner asks you to reject all emails that fail DMARC verifications. Sender of unauthorized email receives rejection notice.

The value of DMARC to policy p=none (Monitoring)

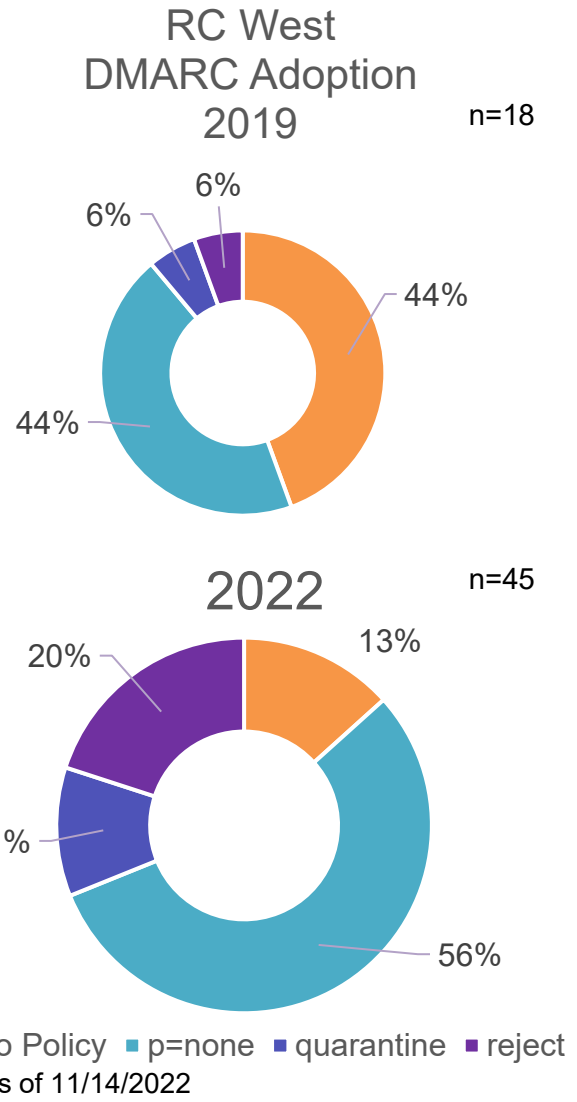
- This policy setting is the starting point for all DMARC implementations, and is the least restrictive policy.
- By setting your policy to p=none, you're asking the receiving domains to handle mail as they normally would and to not take any additional action on mail that could fail authentication.
- At p=none you will begin to receive daily aggregate reporting from participating ISPs detailing a number of items, such as the number of messages they've seen using your domain name, how many messages passed or failed authentication, and authentication results of the mail.
- Passed or failed authentication can be used by the receiving party to evaluate the likelihood of a phishing email. Example:

DMARC Policy Mix and the end of each year



DMARC Adoption @ RC West

- 87% of RC West participants (45 assessed) have started DMARC implementation:
  - Improvement compared to 2019 (56% of 18)
  - 31% (14) have DMARC Policy reject or quarantine (2019: 12%)
  - 56% (25) have DMARC Policy p=none
- **Call for Action:**
  - Remaining 13% (6): please start DMARC implementation and set initial policy (<1 day effort)
  - Require your vendors to have a DMARC policy in place



DMARC Adoption @ RC West – Status as of 11/14/2022

- Quarantine or Reject (14)

Company	DMARC Policy
APS	Quarantine
Avista	Reject
BPA	Reject
CAISO	Quarantine
CENACE	Quarantine
Grant PUD	Quarantine
Los Alamos - NNSAL	Reject
Montana Alberta Tie Line	Reject
NaturEner USA	Quarantine
NV Energy	Reject
PacifiCorp	Reject
Salt River Project	Reject
SPP	Reject
WAPA	Reject

- No DMARC policy (6)

Company
Avangrid Renewables
Douglas County PUD
Eugene Water and Electric Board
Modesto Irrigation District
Public Service Co. of New Mexico
WECC

DMARC Adoption @ RC West – Status as of 11/14/2022

- Monitoring, p=none (25)

Company
AEPCO - AZ Electric Power Coop
AESO
BANC-SMUD
BCHA
Chelan PUD
Hetch Hetchy
Idaho Power
IID
LADWP
Lone Star Transmission, LLC
NorthWestern Energy
PG&E
Portland General Electric
Puget Sound Energy
Redding Electric
SCE
SDGE
Seattle City Light
Silicon Valley
Snohomish County PUD
Tacoma Power
Trans Bay Cable
Tri-State
Turlock Irrigation District
Valley Electric Association

Summary & Next steps

- DMARC helps reduce risk of phishing attacks, the most widely used attack vector, by preventing email spoofing
- DMARC has been widely adopted, US agencies have fully implemented DMARC
- DMARC in lowest policy setting (Policy p=none) helps reduce risk with low cost of implementation
- 87% RC West members have started implementation, 31% fully implemented

Next steps

- Call for voluntary adoption of DMARC within RC West and electric industry in general
- Require vendors to have a DMARC policy in place.

Back-up Information

IMPLEMENTING DMARC BEST PRACTICES

Implementing DMARC – Overview

1. Deploy SPF or DKIM. For 100% alignment, both must be implemented.
2. Create a DMARC record in DNS and set the “Monitor” flag in the record (p=none).
3. Set a value for the RUA value of the DMARC record to receive aggregate reports for the domain.
4. Set a value for the RUF value of the DMARC record to receive forensic reports for the domain. These are especially valuable because they provide more granular detail about the message and the path it traveled.
5. Review and confirm all Mail/Message Transfer Agents (MTA) which use the sending domain are aligned properly using SPF and DKIM. This may be the most tedious step of the process.
6. Review and Observe reports to confirm all senders are in alignment and adjust SPF and/or DKIM as needed.
7. Update the DMARC record to a policy of Quarantine (p=quarantine). Review and make any adjustments as needed.
8. Move to Reject (p=reject).

Implementing DMARC – Sender Policy Framework (SPF)

Deploy SPF to define authorized senders. Example for caiso.com:

V=spf1 mx:caiso.com ip4:50.18.250.17 –all

Prefix	Type	Value	Description
v	version	Spf1 (v=)	The SPF record version.
The result of the check will show one of the following prefix's: "+" Pass: The SPF record states the host is permitted to send. "-" Fail: The SPF record states the host is NOT permitted to send. "~" SoftFail: The SPF record states the host is not permitted to send but is in transition. "?" Neutral: The SPF record states explicitly that no judgement is made on the validity of the host.	mx	caiso.com (mx:)	MX defines all 'A' records to be tested in order of priority. The condition passes if the client IP is found in them.
The result of the check will show one of the following prefix's: "+" Pass: The SPF record states the host is permitted to send. "-" Fail: The SPF record states the host is NOT permitted to send. "~" SoftFail: The SPF record states the host is not permitted to send but is in transition. "?" Neutral: The SPF record states explicitly that no judgement is made on the validity of the host.	ip4	50.18.250.17	Match if IP is in the given range. An ip6 address can also be specified.
The result of the check will show one of the following prefix's: "+" Pass: The SPF record states the host is permitted to send. "-" Fail: The SPF record states the host is NOT permitted to send. "~" SoftFail: The SPF record states the host is not permitted to send but is in transition. "?" Neutral: The SPF record states explicitly that no judgement is made on the validity of the host.	all	all	Always matches. It goes at the end of your record. If the condition does not match, the result fails. To specify a **softfail**, create an SPF record that uses (~all) instead of (all). This will allow for some fails to continue to be processed.

For more information please visit http://www.open-spf.org/SPF_Record_Syntax/

Implementing DMARC – DomainKeys Identified Mail (DKIM)

DKIM provides domain-level digital signature authentication. This is a combination of public key cryptography and Domain Name Service (DNS). Example for caiso.com:

v=DKIM1; p=<encoded base 64>

Tag	TagValue	Name	Description
v	DKIM1	Version	The DKIM record version
p	string	Public Key	Public-key data. The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.

Important note - *"A common view about a DKIM signature is that it carries a degree of assurance about some or all of the message contents, and in particular, that the RFC5322.From field is likely to be valid. In fact, DKIM makes assurances only about the integrity of the data and not about its validity. Still, presumptions of the RFC5322.From field validity remain a concern. Hence, a signer using a domain name that is unrelated to the domain name in the RFC5322.From field can reasonably expect that the disparity will warrant some curiosity, at least until signing by independent operators has produced some established practice among recipient Assessors."*

-**Source**: https://datatracker.ietf.org/doc/rfc5863/?include_text=1 *Section 2.4; "Recipient-Based Assessments"*

For more information please visit http://www.dkim.org/

Implementing DMARC – Create the DMARC record

Test both SPF and DKIM prior to deploying the DMARC record then proceed as necessary. Example caiso.com:

v=DMARC1; p=quarantine; fo=1; rua=mailto:dmarc_rua@caiso.com; ruf=mailto:dmarc_ruf@caiso.com

Recommendation: start with p=none until all sending IP's are included into the SPF record.

Tag	TagValue	Name	Description
v	DMARC1	Version (v=)	Identifies the record retrieved as a DMARC record. It must be the first tag in the string.
P	quarantine	Policy (p=)	Policy to apply to email that fails the DMARC test. TagValue can be 'none', 'quarantine', or 'reject'. This tells the recipient domain how to process the message.
Fo	1	Forensic Reporting (fo=)	Forensic reporting options. The value of this tag is a colon-separated list of characters. Possible values: (0) to generate reports if all underlying authentication mechanisms fail to produce a DMARC pass result, (1) to generate reports if any mechanisms fail, (d) to generate report if DKIM signature failed to verify, (s) if SPF failed. If no ruf tag is specified, this tag will be ignored.
Rua	*mailto:dmarc_rua@caiso.com*	Receivers (rua=)	List of URIs for receivers to send XML feedback to. URIs are required to be added in the format of 'mailto:address@example.com'.
Rruf	*mailto:dmarc_ruf@caiso.com*	Forensic Receivers (ruf=)	List of URIs for receivers to send Forensic reports to. URIs are required to be added in the format of 'mailto:address@example.com'.

For more information please visit https://dmarcguide.globalcyberalliance.org/#/

Implementing DMARC – Tips for Success

Know your senders!

- Take special care in observing the result of setting the DMARC record in monitoring mode.
  - This ISO had great success in identifying senders who may be impacted during the DMARC process by incorporating input from both InfoSec and the Business Units. More specifically during SPF and DKIM phases. The likelihood of daily business or individual process impact when moving to an actionable policy is of note (Ex.Ticketing Services/Notification systems/ListServ groups).

Do your Vendors/Business Partners support DMARC?

- In a few cases, some vendors did not support DMARC or felt that DMARC was not an availability/delivery priority for there service. This may lead to a delay in moving to an actionable policy.
  - The ISO had great success by incorporating DMARC centric questions into Vendor Risk Assessments/Questionnaire.

What about mail forwarding and/or alteration while in transit?

- It is not uncommon for some organizations mail infrastructure to have many moving parts. Messages are forwarded or altered while in transit which can lead to DMARC failures.
  - The, "IETF's DMARC working group published RFC 8617 Authenticated Received Chain (**ARC**) protocol on July 9, 2019" – Source: https://dmarc.org/2019/07/arc-protocol-published-as-rfc-8617/. More information can also be found on the DMARC website.

DMARC Requirements: No Exceptions

- The "v=DMARC1" is the first string in the record
- The policy tag "p=" will always follow the "v=" tag
- The string "DMARC" must always appear in capital letters
- Be careful with syntax while entering records into DNS. Some platforms may vary.

Beware the TempError

- Pay special attention to any TempError failures. These are most likely a DNS cache issue that may cause deliverability issues if not resolved early on.
  - The ISO had success in reviewing the current cache settings and reviewing mail flow as it applied to DNS.