“When security risks in web services are discovered by independent security researchers who understand the severity of the risk, they often lack the channels to properly disclose them.

As a result, security issues may be left unreported. Security.txt defines a standard to help organizations define the process for security researchers to securely disclose security vulnerabilities.”

```
# https://example.com/.well-known/security.txt

Contact: security@domain.com
Contact: +65 1234 5678
Contact: https://example.com/security-policy

Encryption: https://example.com/pgp-key.txt

Signature:
-----BEGIN PGP SIGNATURE-----
...
-----END PGP SIGNATURE-----
```

Why security.txt?

A concise point-solution to the need of reporting security issues, building on existing conventions such as robots.txt and the security@ email address standard.

SECURITY.TXT IS PUBLICLY ENDORSED BY

Going forward...

- We have not identified competing proposals
- The standard has been channeled in multiple discussion forums and been developed based on the feedback
- The convention is seeing adoption already, indicating approval
- It has come to our attention that companies are *waiting to adopt security.txt until it becomes standard*

→ **Our proposal is to form a working group and make this an IETF RFC.**