Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India

Policy Brief

Published January 23, 2019 (Updated March 20, 2019)

By **Karan Saini, Pranesh Prakash** and **Elonnai Hickok**

Research Assistance by **Pranav M B**

Legal Analysis by **Gurshabad Grover**

Edited by **Gurshabad Grover**

The Centre for Internet and Society, India

Acknowledgments

We would like to thank **Srinivas Kodali, Aseem Jakhar, Manu Zacharia, Akash Mahajan** and **Rahul Sasi** for their invaluable insights and contributions.

We would also like to thank **Anand V** and **Pukhraj Singh** for providing us with their feedback on a previously published version of this brief.

Executive Summary

The aim of this policy brief is to recommend changes pertaining to current legislation, policy and practice to the Government of India regarding external vulnerability reporting and disclosure. The changes we recommend within this brief aim to strengthen the processes around voluntary vulnerability and bug disclosure by third parties. The proposed changes also aim to improve the current scope for interaction between members of the security community and the Government.[1]

The ubiquitous adoption and integration of information and communication technologies in almost all aspects of modern life raises with it the importance of being able to ensure the security and integrity of the systems and resources that we rely on. This importance is even more pressing for the Government, which is increasing its push of efforts towards digitising the operational infrastructure it relies on, both at the State as well as the Central level.

This policy brief draws from knowledge that has been gathered from various sources, including information sourced from newspaper and journal articles, current law and policy, as well as from interviews that we conducted with various members of the Indian security community. This policy brief touches upon the issue of vulnerability disclosures, specifically those that are made by individuals to the Government, while exploring prevalent challenges with the same and making recommendations as to how the Government's vulnerability disclosure processes could potentially be improved.

Key learnings from the research include:

- There is a noticeable shortcoming in the availability of information with regard to current vulnerability disclosure programmes and process of Indian Government entities, which is only exacerbated further by a lack of transparency;
- There is an observable gap in the amount and quality of interaction between security researchers and the Government, which is supported by the lack of proper channels for mediating such communication and cooperation;
- There are several sections and provisions within the Information Technology Act, 2000, which have the potential to disincentivise legitimate security research, even if the same has been carried out in good faith.

[1] An earlier version of this paper included a brief discussion on the potential benefits of India formalising a Vulnerability Equities Process ("VEP") framework. Following the initial publication of the paper we received significant feedback on our inclusion of the topic within the paper. The brief inclusion of VEP has since been removed as the authors believe that it digresses from the central focus of the paper, which is on Coordinated Vulnerability Disclosure, while also considering that the limited scope of the current paper does not give VEP the requisite amount of scrutiny and attention. Our recommendations on VEP, along with its potential and criticism will be discussed in an upcoming paper.

Definitions

This section provides a brief taxonomy of the various terms that are used throughout or are otherwise relevant to the brief:

- **Vulnerability Disclosure**[2] traditionally refers to the practice of providing the vendor or provider of a particular software library or package, hardware component, or a product or service, with information about security vulnerabilities, bugs or other flaws that may affect said software, hardware, product or service.
- **Coordinated Disclosure**[3] traditionally refers to a practice wherein the individual responsible for discovering a particular security vulnerability or issue withholds public disclosure of the flaw until the affected vendors or providers have had the opportunity to patch the vulnerability
- **Full Disclosure**[4] traditionally refers to the practice wherein the individual responsible for discovering a particular security vulnerability or flaw believes that user interest would be better served if specific details of the discovered vulnerability were impartially disclosed in a simultaneous manner to the general public as well as the vendor. Full Disclosure may also refer to breaking adherence to the stipulations of Coordinated/Responsible Disclosure, say for instance, in cases where the individual responsible for discovery of a particular flaw believes that the vendor or service provider has not adequately upheld their responsibility to mitigate or otherwise address the issue.
- **Non-Disclosure**[5] traditionally refers to the practice wherein the individual responsible for discovering a particular security vulnerability or flaw does not disclose the details or existence of the particular flaw to the vendor or service provider. The reasoning for adhering to this practice can vary, however, in some cases, non-disclosure may stem from the discovering wanting to later exploit the discovered flaw.
- **Bug Bounty Programs**[6] traditionally refers to independent or managed vulnerability disclosure programs wherein the external discovery and subsequent disclosure of a legitimate security flaw (in a coordinated manner) is rewarded by the vendor. The reward (or "bounty") for a legitimate discovery is traditionally monetary.

[2] "Software Vulnerabilities" by Cencini et. al. https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf

[3] MSRC Coordinated Vulnerability Disclosure https://www.microsoft.com/en-us/msrc/cvd

[4] ibid

[5] ibid

[6] https://www.mozilla.org/en-US/security/bug-bounty/

Introduction

The presence of security vulnerabilities and flaws in any type of digital technology is virtually unavoidable. While there are a wide array of best practices which can be adopted in an effort to minimise the presence of security vulnerabilities (ISO 27034[7] and OWASP[8]), adherence to best practices and standards still cannot act as an "end-all" to or eliminate entirely the prevalence of security vulnerabilities or flaws within a particular system or technology.

As the security landscape is continually evolving, new attack vectors and surfaces are constantly discovered by both malevolent actors as well as hackers who undertake their exploratory research in good faith. In the case of the latter, details of the discovered security flaws are usually disclosed to the affected developer or provider of the particular software or service. This is followed, at times, by public disclosure of the discovered flaw. Public disclosure usually only happens either after a patch has been issued by the vendor responsible. In certain cases, where the stipulated timeline for mitigation of the issue has passed, public disclosure may happen prior to a patch being deployed. Public disclosure is traditionally practiced in an effort to educate the users of a particular service or technology of existing security flaws, as well as to inform better design practices for similar protocols and/or technologies in the future.

Considering that security issues can not always be avoided and may be missed during development and testing stages, the ideation and implementation of a vulnerability disclosure program or policy that leverages the expertise of members of the security community becomes extremely crucial. The "crowdsourced model" which vulnerability disclosure and bug bounty programs employ can be instrumental for continuous mitigation of security flaws. The vulnerability disclosure and handling processes can briefly be described as, "*formal internal mechanisms for receiving, assessing, and mitigating security vulnerabilities submitted by external sources, such as independent researchers acting in good faith, and communicating the outcome to the vulnerability reporter and affected parties.*"[9]

As use of (and reliance on) digital technologies becomes more and more prevalent, the scope for potential security flaws to exist is effectively also widened, and as such, it becomes harder to ensure the integrity and security of the systems that reliance is placed on. This problem affects all levels of governance within the country and is be caused by a variety of factors, including: inadequate technological infrastructure, lack of awareness or adherence to security practices, standards and guidelines, lack of utilisation of existing resources (including human talent), among many others.

Additionally, when considering the ecosystem which is affected, even conceptualising or defining the scope of the issue becomes quite difficult, given especially how widespread the use of digital technologies has become for purposes of Governance. We believe that it would be useful for the Indian Government to adopt a holistic approach to mitigating potential security flaws within their technological infrastructure, such as by drawing from the vast pool of available resources and talent,

[7] ISO 27034 provides a framework and guidelines for specifying, designing and applying application security controls - **http://www.iso27001security.com/html/27034.html**

[8] Open Web Application Security Project is a joint effort led by members of the security community.
The project provides an array of information on various topics relating to application security - **https://www.owasp.org/index.php/Main_Page**

[9] Joint comments to NIST Framework (Revision 1.1)
https://www.nist.gov/sites/default/files/documents/2017/05/12/2017-04-10-consortium.pdf

which, for the purposes of this policy brief, includes the expertise of members of both the Indian as well as the global security community, which consists of professionals, hackers, researchers, practitioners and enthusiasts alike.[10]

Methodology

For the purpose of this policy brief, we focused on the existing scope for interaction and cooperation between members of the security community and various Government entities, mainly to examine how the practices of voluntary vulnerability reporting and disclosure have been shaped so far by policy, legislation and practice.

Questions which this brief reflects on include:

1. What hurdles do hackers face when disclosing vulnerabilities to the Government, and in engaging in security research?
2. How can the existing frameworks for voluntary vulnerability reporting and disclosure be improved?
3. Is the present legislative framework conducive to a vibrant culture for security researchers and hackers?

These questions warrant discussion on three critical issues:

1. Processes: Current and future systems and processes which allow for security vulnerabilities to be disclosed to Government entities;
2. Collaboration: Systems and processes which enable and enhance interactions between hackers and the Government;
3. Legislative Frameworks: Legislative frameworks which serve the purpose of enabling legitimate security research.

The research inputs for this policy brief were gathered from the following sources:

1. Interviews with members of the Indian security researcher community that primarily focused on their experiences in disclosing vulnerabilities to the government (specifically the available avenues for disclosure and the responses received), as well as how the ecosystem could be improved; [11]
2. Newspaper and journal articles, along with materials produced by security practitioners, private companies and foreign Governments;
3. Analysis of currently applicable law and policy.

[10] Throughout this document, we refer to members of the security community as “researchers” and “hackers” interchangeably. It should be noted that our use of the term “hacker” is without any of the distinctions which usually precede it (such as “ethical” or “whitehat”) since those terms aren’t very meaningful and often lead to confusion.

[11] The names of the individuals that we interviewed can be found in the “Acknowledgements” section of the report. We were unable to source on-the-record interviews with Government officials.

Current State of Vulnerability Reporting in India

Currently in India, there seem to be four entities which actively accept vulnerability reports from third parties with regard to Government and other sensitive information infrastructures, namely: the Indian Computer Emergency Response Team (CERT-IN),[12] the National Informatics Centre Computer Emergency Response Team (NIC-CERT),[13] the National Critical Information Infrastructure Protection Centre (NCIIPC) as well as the Cyberdome initiative of the Kerala Police.[14]

The table below outlines information that is available about the entities responsible for receiving and acting on vulnerability reports, while also highlighting the information that we were unable to find in our research.[15]

Body	Legislative Backing	Format for Report Submission	Types of Reports Accepted	Support for Encrypted Submissions	Year Established
NCIIPC	Information Technology Amendment Act, 2008	*Email*	Incident, Malware and Vulnerability Reports	No	January 2014
CERT-IN	Information Technology Amendment Act, 2008	*Phone and email*	Incident and Vulnerability Reports	Yes	January 2004
NIC-CERT	N/A	*Phone and email*	Incident and Vulnerability Reports	No	December 2017
Kerala Police Cyberdome	N/A	*Web form*	N/A	No	August 2014

[12] CERT-IN provides reporting mechanisms for security incidents: **http://CERT-IN.org.in/SecurityIncident.jsp** and for vulnerabilities: **http://CERT-IN.org.in/VulnerIncident.jsp**

[13] National Informatics Centre Computer Emergency Response Team - **https://nic-cert.nic.in/index.jsp**

[14] Kerala Cyberdome - Report A Suspicious Activity in the Cyber Space
http://www.cyberdome.kerala.gov.in/reportus.html

[15] While these entities solicit, accept and coordinate the task of resolving vulnerability reports that are submitted by third parties, they do not run or maintain full-fledged, formalised and coordinated vulnerability disclosure programmes.

Difficulties Faced in Reporting Vulnerabilities

All of the hackers that we interviewed noted several challenges in reporting security vulnerabilities to the Government without exception. The difficulties are manifold:

1. **Process**: It was noted that in some cases, it is difficult to identify whom to report a particular security vulnerability to, considering that Government websites in India do not, as a standardised framework and practice, include contact information for the submission of security vulnerabilities. Further, even when a website does have a “Contact Us" section, the process for vulnerability disclosure is usually unclear and open ended. Individuals do not know whether their report will reach a person or team that can comprehend and take action on the report, or if it will be acted upon. Furthermore, when reporting security flaws to any of the four entities named above, there appears to be a lack of clarity on the hierarchy of jurisdiction which would dictate when an issue affecting a particular Government website is to be reported to a particular entity.

2. **Communication**: The lack of clarity on what happens to a vulnerability report after it is submitted poses an additional barrier to security researchers. This results in a situation where security researchers invest a significant amount of time and effort to first report a vulnerability and then repeatedly attempt to follow up on whether it has been fixed. It is important to note, however, that this situation is not always the case, as multiple interviewees noted that they have had positive and timely resolutions when reporting security issues to the NCIIPC. The interviewees also stated that their interactions with the NCIIPC could set a good example for other Government entities that are responsible for receiving and acting on vulnerability reports.

3. **Accessibility**: The process of submitting details regarding security flaws can sometimes itself pose a challenge. While the Kerala Cyberdome provides a web-based form which seemingly allows for the submission of security vulnerabilities and flaws,[16] NCIIPC,[17] CERT-IN[18] and NIC-CERT[19] provide static PDF forms which have to be downloaded, filled and sent via physical post or email. One interviewee in particular felt that the forms provided by the NCIIPC for vulnerability reporting were aimed towards Government *“insiders”,* as the form includes several fields which, the interviewee believes, only Government IT officials would know how to fill. It would greatly streamline the vulnerability disclosure process if entities such as NCIIPC and CERT-IN also provided web-based forms for the submission of vulnerability reports. Considering that such forms could also embed conditional logic (i.e., displaying specific questions based on previous responses), they could potentially provide for a more meaningful reporting structure in comparison to the currently used static form. We also recommend that the pages and forms which facilitate vulnerability disclosure are made available in a variety of Indic languages for increased accessibility. At the same time, a novel method of vulnerability and incident reporting provided by some of the above mentioned entities is that of a telephone-based helpline,[20] which has the potential to act as a much

[16] Reporting Page, Kerala Police Cyberdome **http://www.cyberdome.kerala.gov.in/reportus.html**

[17] NCIIPC Vulnerability Disclosure Form **http://nciipc.gov.in/documents/Vulnerability_Disclosure_Form.pdf**

[18] CERT-IN Vulnerability Disclosure Form **https://CERT-IN.org.in/PDF/Vul_Report.pdf**

[19] NIC-CERT Vulnerability Disclosure Form **https://nic-cert.nic.in/pdf/Vulnerability%20Reporting%20Form.pdf**

[20] NCIIPC (1800-11-4430, retrieved from **http://nciipc.gov.in/RVDP.html**), NIC-CERT (+91-11-2290-2400, retrieved from **https://nic-cert.nic.in/index.jsp**)

faster alternative when compared to traditional email communication. However, it should be noted that none of the hackers we interviewed commented on the use or efficacy of this measure.

Motivations for Reporting Vulnerabilities to the Government

On the basis of the interviews we conducted with members of the Indian security community, multiple factors which may motivate individuals to report security flaws to the Government came to light:

1. **Mitigation of Reported Vulnerabilities**: Our first and perhaps most important learning was that individuals who report security issues to the Government unconditionally wish to see the flaws mitigated. Several of the hackers we spoke to described their voluntary disclosure of security flaws to entities such as NCIIPC and CERT-IN as that being done out of a sense of *"duty"*. However, as noted above, while some entities are responsive to vulnerability reports received from external sources, others are not. The NCIIPC was one such entity that was noted as being responsive by some our interviewees. One interviewee asked, *"what happens after [submitting] the report? I don't get to know"*. He noted that, *"some of the vulnerabilities I find are common across departments, and [as such] it is unclear whether the reports I submit end up resulting in any form of coordinated action"*. Another interviewee noted that, *"sometimes they don't even read [the reports], and sometimes, they do read them [but instead] don't acknowledge [them]"*.

2. **Acknowledgement and Recognition**: The second most important aspect in terms of motivations for voluntary vulnerability disclosure is recognition or acknowledgement by the Government. As one interviewee noted, Government entities need "*to tell the hacking community that they are approachable, and that if [hackers] have something [to report], they are happy to fix it and provide some form of recognition."* The interviewee suggested that official Government handles on Twitter could perhaps share a note of gratitude acknowledging the individual, as that might be all that a reporting party is seeking. Another interviewee suggested that a *"thank you email"* or a *"security hall of fame"* page on a Government website may also fulfill this motivation by providing due credit and acknowledgement to the individual responsible for reporting a particular vulnerability. Another interviewee spoke of *"some form of recognition with [an] official seal"*, such as a certificate or letter, which he surmised would be enough to satisfy most younger hackers. A security researcher who had discovered simple flaws across a range of Indian diplomatic websites and reported them to the Ministry of External Affairs, had requested for a token payment apart from some form of acknowledgement. It would perhaps be useful to develop a system which provides public acknowledgement and recognition to reporting parties, since many security researchers might not necessarily be looking for monetary compensation when it comes to the Government, preferring instead to receive compensation for similar work from the private sector.

It is clear that there is a need for vulnerability reporters to be informed when their reports have been lodged, it might also be beneficial to perhaps provide security researchers with the status of their report, including information on whether it has been received, triaged and ultimately mitigated.[21] It is also clear that there is a need for increased oversight and accountability into the functioning of entities that are tasked with receiving and responding to vulnerability reports. Government entities can also further incentivise their vulnerability disclosure processes by creating a platform which can be used to publicly acknowledge contributions made by individuals that have submitted legitimate vulnerability reports, as currently, none of the above mentioned entities host a dedicated “acknowledgement” or “security hall of fame” page on their websites.

Ensuring Confidentiality of the Vulnerability Disclosure Process

Our research found that, out of the pool of Government entities that are tasked with receiving and responding to vulnerability reports from external parties, some entities themselves fail to take adequate measures when it comes to maintaining the integrity and/or confidentiality of their services. NCIIPC makes use of an untrusted SSL certificate issued by (n)Code Solutions, which is a subsidiary of the Government-owned Gujarat Narmada Valley Fertilizers and Chemicals Limited. The SSL certificate does not work as intended on most browsers due to the fact that the issuer is not a recognised or trusted Certificate Authority (“CA”). This may be due in part to the fact that Indian Government Certificate Authorities have been used in the past, either by third party actors or malicious insiders, for the creation of SSL certificates attempting to impersonate the domains of companies such as Google and Microsoft.[22]

The Kerala Police Cyberdome website, too, does not support HTTPS.[23] This lack of use of cryptography can allow for interception to be carried out by (potentially malicious) third parties. At the very least, Government entities which facilitate the transmission of sensitive information from visitors - which should be the default classification category for vulnerability reports - should as a standard requirement and practice make use of TLS.

Ensuring that vulnerability reports are **a)** delivered to relevant entities in a secure manner and that **b)** they are not intercepted or tampered with is a critical part in ensuring the integrity of current vulnerability disclosure processes. If interception is possible, potentially malicious third parties would be in a position to discover information about unpatched security flaws, and as a result, gain the ability to exploit them before a fix is deployed.

Further, while NCIIPC makes use of the NIC email server (which provides transport-layer email encryption, i.e., encryption of the connection between their own email server and those of others, offering limited security guarantees),[24] the email server for CERT-IN does not support transport-level encryption. Additionally, while it is notable that CERT-IN does allow for PGP encrypted

[21] Ironically, vulnerability trackers themselves need to be guarded against vulnerabilities that allow information about unpatched vulnerabilities to leak.
https://threatpost.com/flaw-in-google-bug-tracker-exposed-reports-about-unpatched-vulnerabilities/128687/

[22] "In the Wake of Unauthorized Certificate Issuance by the Indian CA NIC, can Government CAs Still be Considered ‘Trusted Third Parties’?" **https://casecurity.org/2014/07/24/unauthorized-certificate-issuance/**

[23] SSL Labs SSL Test for Kerala Police Cyberdome Website
https://www.ssllabs.com/ssltest/analyze.html?d=cyberdome.kerala.gov.in

[24] While NIC's "mailgw.nic.in" email gateway allows for transport-layer encryption, the certificate they use is in the name of "*.emailgov.in", and is not valid for "mailgw.nic.in". This prevents any person from being sure that they are indeed communicating with mailgw.nic.in without any interception.

communication to be sent to their vulnerability submission email address, the public key required to encrypt messages to the organisation is not easy to locate. The public key is not made available on the homepage of the entity's website, or even on the page which facilitates vulnerability disclosure from third parties,[25] rather it is available on the "Contact Us" section of their website. Finally, it was also found that none of the other three entities that are tasked with receiving and acting on vulnerability reports have published their public keys on their websites. It is therefore recommended, specifically for entities which are in charge of receiving and acting on vulnerability submissions to **a)** allow for incoming communication to be encrypted and **b)** ensure that their public keys are easy to locate and access.

Standards on Vulnerability Disclosure and Resolution

Standards are imperative for ensuring consistency throughout the processes and practices that are followed across different organisations. First proposed in the year 2005 (and after a decade of work involving collaboration with multiple stakeholder groups), the International Organization for Standardization ("ISO") published two standards in the year 2014: ISO 29147 - which deals with vulnerability disclosure[26] and ISO 30111 - which deals with processes for handling security vulnerabilities.[27] Additionally - unlike most of the other technical standards that have been published by the International Organization for Standardization - ISO 29147 can be accessed completely free of cost.[28]

The ISO 29147 standard covers guidelines which are to be followed by vendors and service providers when dealing with vulnerability reports submitted by "external finders" (i.e., security researchers), while also covering other aspects, such as the subsequent release of information to customers or users of the particular product or service with regard to the discovered vulnerabilities. ISO 30111 (which, unlike ISO 29147 is not available freely) covers the processes that are to be followed for "handling" vulnerability reports, including those submitted by both external and internal finders - along with information on how to verify and resolve discovered vulnerabilities.

While there is a lack of quantitative information on the adoption of these standards, it can be said that, platforms which facilitate and manage vulnerability disclosure and bug bounty programs - such as Bugcrowd[29] and HackerOne[30] - have embraced these standards quite readily.

There are some positive international examples of efforts which have been undertaken to standardise processes around vulnerability disclosure, too. For instance, in 2015, the National Telecommunications and Information Administration ("NTIA")[31] - which is a part of the U.S. Department of Commerce - launched "an initiative to address key cyber security issues facing the

[25] CERT-IN, Vulnerability Disclosure Page **https://CERT-IN.org.in/VulnerIncident.jsp**

[26] ISO/IEC 29147:2018: Information technology - Security techniques - Vulnerability disclosure **https://www.iso.org/standard/72311.html**

[27] ISO/IEC 30111:2013: Information technology - Security techniques - Vulnerability handling processes **https://www.iso.org/obp/ui/#!iso:std:53231:en**

[28] **https://threatpost.com/the-time-has-come-to-hack-the-planet/117419/**

[29] Bugcrowd, Frequently Asked Questions **https://www.bugcrowd.com/resources/for-companies/faqs/**

[30] HackerOne, Vulnerability Disclosure Policy: What Is It, Why You Need One, and How to Get Started **https://www.hackerone.com/sites/default/files/2018-11/vulnerability-disclosure-policy.pdf**

[31] Enhancing the Digital Economy Through Collaboration on Vulnerability Research Disclosure **https://www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure**

digital economy that could be best addressed by a consensus-based multistakeholder process",[32] following an extensive gathering of initial public comments.[33] This initiative has thus far resulted in prominent participation and useful coordination from multiple stakeholders - including stakeholders from the private sector such as Symantec and Rapid7 - as well as from non-profit organisations such as the Electronic Frontier Foundation. The collaboration have so far fruitioned in the form of comments and inputs on vulnerability disclosure and handling processes, along with how these processes could be rolled into the more general Cybersecurity Framework of the US Government.[34]

Vulnerability Reporting in Other Countries

This section examines vulnerability reporting processes and programmes in the U.S., Singapore, and the Netherlands to understand different models and frameworks that have been successful for Governments across the world. The Computer Emergency Response Team of the U.S. states clearly that it accepts both reports relating to vulnerabilities in US Government websites as well as flaws in general software.[35]. The U.S. Department of Defence has also famously tied up with HackerOne[36] in order to launch the "Hack the Pentagon"[37] and the "Hack the Air Force 3.0"[38] challenges in 2015 and 2018 respectively. According to HackerOne, the Department of Defence's Hack the Pentagon initiative led to an impressive participation of more than 1400 hackers, with the first vulnerability report being submitted around 13 minutes after the initial launch of the program.[39] The first iteration of the program was limited only to US citizens, however, since then, the U.S. Department of Defence has started accepting bug submissions made by security researchers from the world over.

The vulnerability disclosure policy of the United States Department of Defense ("U.S. DoD") states that participants "must comply with all applicable Federal, State, and local laws" when attempting to find security vulnerabilities in their systems. The policy also states in clear language that failure to adhere to the laid out guidelines may result in the individual being "subject to criminal and/or civil liabilities." The responsible disclosure programme which the Government of the Netherlands runs also has a similar policy, wherein it is stated that the Government "will not attach any legal consequences" to the vulnerability report or actions related to it as long as **a)** the vulnerability is not disclosed prematurely and **b)** the vulnerability is not exploited unnecessarily (i.e., beyond what may be required to demonstrate its existence and severity).[40]

[32] Multistakeholder Process: Cybersecurity Vulnerabilities **https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities**

[33] Comments on Stakeholder Engagement on Cybersecurity in the Digital Ecosystem **https://www.ntia.doc.gov/federal-register-notice/2015/comments-stakeholder-engagement-cybersecurity-digital-ecosystem**

[34] Consortium Joint Comments to NIST Framework (Revision 1.1) **https://www.nist.gov/sites/default/files/documents/2017/05/12/2017-04-10-consortium.pdf**

[35] Incident Reporting System | US-CERT **https://www.us-cert.gov/report**

[36] HackerOne is a privately owned company which provides organisation with a platform for vulnerability disclosure and bug bounty program management **https://hackerone.com**

[37] HackerOne - Hack the Pentagon **https://hackerone.com/hackthepentagon**

[38] HackerOne - Hack the Air Force 3.0 **https://hackerone.com/htaf3**

[39] "Hack the Pentagon is a bug bounty program of the US Department of Defense on the HackerOne platform" **https://www.hackerone.com/resources/hack-the-pentagon**

[40] Responsible Disclosure | Cybercrime | Government.nl **https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure**

In 2018, the Singaporean Ministry of Defence ("MoD") partnered with HackerOne to launch their own bug bounty programme,[41] which saw participation from over 200 hackers, and subsequently also resulted in the submission and remediation of 35 valid security vulnerabilities.[42] Additionally, the Singaporean MoD has since also announced that it would be hosting another time-bound bug bounty program.[43] While it is clear from the success of MoD's bug bounty program that a time-bound bug bounty event may be useful for securing critical infrastructure, it can be said that allowing for consistent submissions to be made to the Government may also ultimately help forge a more meaningful, long-term relationship of trust between members of the security community and the Government.

Hurdles Posed by the Information Technology Act

There are many provisions in the Information Technology Act, 2000 which pose hindrances to security researchers and hackers due to the use of broad and vague language. Such provisions have the potential to manufacture offences out of activities which are necessary and part of the vulnerability discovery process, including activities such as the probing or scanning of networks and connected machines, altering of computer resources (an activity which may be necessary for some types of vulnerability discovery and research), and even merely accessing computer resources in certain cases, among many others. Such provisions create the potential for error on the part of both law enforcement and the judiciary. The specific provisions in this regard include Section 43[44]

[41] Fact sheet: Ministry of Defence (MINDEF) Bug Bounty Programme **https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2017/december/12dec17_fs**

[42] **https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2018/february/21feb18_fs**

[43] Business Wire, Singapore Government to Launch Second Bug Bounty Initiative with HackerOne to Boost Cyber Defences **https://www.businesswire.com/news/home/20181220006005/en/Singapore-Government-Launch-Bug-Bounty-Initiative-HackerOne**

[44] 3. **Penalty and compensation for damage to computer, computer system, etc.**
If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, or computer resource —

1. accesses or secures access to such computer, computer system or computer network;
2. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
3. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
5. disrupts or causes disruption of any computer, computer system or computer network;
6. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
7. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected.
8. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
9. steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

("Penalty and compensation for damage to computer, computer system, etc."), Section 65 ("Tampering with computer source documents") and Section 66 ("Computer related offences").

Section 43 imposes penalties on a wide range of unauthorized actions to computer systems, networks, and resources. In doing so, the provision creates unclear lines between what is acceptable and what is not, as it does not clarify what may be considered as authorization, neither does it account for situations where authorization may not be taken or explicitly granted (including for example, any of the existing vulnerability reporting processes offered by Indian Government entities) and does not also take into consideration intent, thus having the potential to penalise legitimate actions undertaken as a part of the vulnerability discovery and reporting process. For example, browsing a website and accessing/downloading content is a form of access to a website which is typically is done without any prior explicit permission or authorization - yet, it is plausible that a strict reading of Section 43 would make such an action unlawful. It also imposes penalties on anyone who "introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network" or "destroys, deletes, or alters any information in a computer resource". For security researchers, this section becomes problematic for several reasons. One of the reasons which make Section 43 especially problematic is that, out of the four Government entities tasked with receiving and responding to incident, malware and vulnerability reports, none actually grant any prior explicit authorization to researchers. Additionally, "introduc[ing] or caus[ing] to be introduced any computer contaminant or computer virus into any computer, computer system or computer network" is an overly broad (and thus dangerous) description of an offence — which may make it is possible for the Section to be used in such a way which penalise security researchers acting in good faith — especially when considering the lack of a *mens rea* requirement in the law).

Section 65, which criminalises the alteration, destruction, or concealment of computer source code "which is required to be kept or maintained by law" has the potential to open up room for wrongful prosecution, as it is unclear what harm the section is seeking to prevent. Areas of ambiguity include: the process and criteria by which source code becomes 'protected', as well as the very scope of the term, since the definition provided for "computer source code"[45] within the Act bears very little resemblance to the commonly agreed upon definition of the term, wherein it is used to refer to "the version of software as it is originally written (i.e., typed into a computer) by a human in plain text, (i.e., human readable alphanumeric characters)".[46]

This ambiguity has resulted in numerous instances in which police have registered cases under Section 65 of the IT Act despite there being no involvement whatsoever of computer source code. In *Ramesh Rajagopal v. Devi Polymers Pvt. Ltd*,[47] a case was registered under S. 65 where a false electronic record published on a website was alleged to fall under the definition of "source code".

1. "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

[45] In Section 65 of the Information Technology Act, 2000, "computer source code" is defined as "the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form."

[46] Source code definition by The Linux Information Project **http://www.linfo.org/source_code.html**

[47] Criminal Appeal No. 133 OF 2016 (Supreme Court of India) **http://www.advocatekhoj.com/library/judgments/announcement.php?WID=7332**

This was dismissed by the Supreme Court. In *Kavita C. Das v. Arvind Thakur and Anr.*,[48] a case was registered under Section 65 where the use of an "official ID mail" to view pornography was alleged to constitute altering of source code. This was also dismissed by the Court. In *Syed Asifuddin And Ors. vs The State Of Andhra Pradesh*,[49] the Andhra Pradesh High Court interpreted the "or" in "kept or maintained" to be disjunctive, essentially waiving the requirement that was interpreted to be that the source code has to be "kept or maintained by law". Problematically, the Court held that changing the Electronic Serial Number (ESN) of a mobile handset manufactured by a private company amounted to alteration of "computer source code", and thus an offence under Section 65. Such broad interpretations of the law also disincentivise responsible security and vulnerability research.

Section 66 penalises with imprisonment or fine any person that dishonestly or fraudulently undertakes any action prohibited under Section 43. Section 66 exacerbates offences defined in Section 43 by causing them to be criminal wrongs. For instance, if the terms of service of a website prohibits using a script to automate the downloading of publicly available files, then it might be seen as a violation of Section 43 if an individual were to use automation tools to download files from the website - even though the terms of service is only a contractual document and not a binding law. This section may be read as giving people the power to make unilateral terms of service legally binding even without a clickwrap agreement. Further, it would also be a criminal wrong under Section 66 if the use of an automation tool - for instance for scraping a website - was found to have been done in an effort to cause "wrongful loss or wrongful gain" or with an "intent to defraud". The section has the potential deter security researchers from undertaking activities that are both a part of and are critical to the vulnerability research and discovery process. This deterrence is due mostly to the palpable concerns which arise out of the text, with regard to misinterpretation or misconstruing of intent.

Section 66F (B), which

- criminalises knowingly or intentionally penetrating or accessing a computer resource
- without authorisation
- that is restricted for reasons related to the security of the state or with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality,
- or in relation to contempt of court, defamation or incitement to an offence,
- or to the advantage of any foreign nation, group of individuals or otherwise.

can be used to penalize the activities of security researchers as it does not create a process of authorization for them to carry out security or vulnerability research. The broad grounds of misuse listed in the provision (including terms such as decency, morality, defamation, etc.) could also result in most public disclosures of security vulnerabilities being construed as violations of the provision - as they could potentially be viewed as attempts to defame a particular department or Government entity - or to give advantage a foreign nation.

Section 70, which criminalises attempts to gain access to systems that have been notified as "critical information infrastructure" ("CII") under the section also does not contain an exception for security researchers who wish to probe, discover and submit disclosures for security vulnerabilities in CII.

[48] Criminal Misc. No. M-29516 of 2010 (Punjab and Haryana High Court) **https://indiankanoon.org/doc/20805777/**

[49] Criminal Misc. No. 96 of 2006 (Andhra High Court) **https://indiankanoon.org/doc/1459676/**

This criminalisation is in stark contrast to the vulnerability reporting facilities that have been made available by entities such as the NCIIPC and NIC-CERT and could potentially be used to prosecute the actions of security researchers. This potential is further exacerbated largely due to the lack of a formally defined scope and associated rules of engagement for vulnerability discovery and disclosure being put out by Government entities.

Recommendations

From the above discussion, the following recommendations around the existing scope, structure, and implementation of vulnerability disclosure programmes in India can be concretised:

1. **Harmonising Existing Processes:** Through our research it was evident that the Government needs to harmonise existing processes to improve the current state of voluntary vulnerability reporting and disclosure in the country. We recommend the following changes:

    - **Improving Availability of Information on Guidelines and Processes:** It is key that information about the processes, guidelines as well as general details about the functioning of entities currently tasked with receiving and acting on vulnerability reports is available to the public. At a minimum, we would recommend the following information to be made publicly available:

        - **Scope and Authority:** The entities which allow external parties to report security flaws in Government infrastructure currently appear to overlap in terms of organisational hierarchy. This is partly due to the lack of concretisation of a formal scope for the roles and responsibilities of each of the four entities mentioned in this brief. In order to make the vulnerability disclosure processes of each Government entity more comprehensive, it would be desirable that they each formalise a roadmap and high-level scope for their functioning.

        - **Processes:** The process of reporting vulnerabilities to each particular organisation should be prescribed from start to finish. Information on the detailed scope of a particular entity, guidelines for reporting, *"Do's and Don'ts"* and associated legal frameworks, as well as estimated time frames for actions such as first response, triage, and ultimately resolution should be part of what is made known to security researchers.

        - **Statistical Information:** Information about the number of vulnerability reports received by each body, as well as the number of reports that have been resolved should be made publicly available. It may also be useful to include the average time taken from initial response, triage and ultimately the deployment of a fix.

        - **Oversight and Accountability**: It is unclear whether bodies such as CERT-IN, NIC-CERT and NCIIPC are held accountable for ensuring proper receipt and subsequent resolution of vulnerability report submissions. At the very least, the release of high level, non-sensitive information regarding the same may also help increase trust in the entities and their processes.

2. **Improving Interactions Between Security Researchers and the Government**: Through our research, it was clear that there is a clear need to enhance the quality of interactions that take place between members of the security community and the Government entities which they report issues to. We recommend the following improvements which can strengthen the relationship between the two:

    - **Communication of Status:** The following should be communicated by Government entities when dealing with vulnerability report submissions: (i) Acknowledgement confirming receipt of report, (ii) Acknowledgement of the particular flaw upon confirmation of its existence, (iii) Estimated time for fix to be deployed, (iv) Steps that have been taken to address the flaw.

    - **Incentivising Disclosure:** Government entities should actively work to incentivise the submission of vulnerability reports from security researchers through means such as:
        - Public acknowledgement through means of a “security hall of fame”
        - A certificate or letter with an official Government seal
        - Invitation to private vulnerability disclosure and time-bound bug bounty programmes, hackathons or similar events
        - Public acknowledgement through a mention from an official Twitter handle

    - **Awareness and Outreach:** Improved outreach can help make security researchers aware of the Government’s efforts to work with them and effectively increase participation. To the same effect, Government entities may also perform outreach by increasing the level and frequency of their participation in local and international community bodies, as well as community focused security conferences and events.

3. **Improve Current Reporting Processes:** Through our research, it was clear that several aspects of the current process of reporting security vulnerabilities to Government entities could be expanded and improved upon. The following recommendations aim to improve the current processes surrounding the same:

    - **Bug Tracker:** An internal system for tracking and management of vulnerability report submissions may be useful. It can additionally allow for updates to be provided to the reporter(s) of security vulnerabilities, while also making the process of tracking and managing such issues easier for the people that are responsible for addressing them.

    - **Improving Accessibility of Reporting Forms:** It would greatly benefit the vulnerability reporting processes of Government entities if they also provided web-based forms for the submission of vulnerability reports. Considering that such forms could also embed conditional logic (i.e., showing questions based on previous responses), they could potentially provide an efficient and more useful reporting structure in comparison to the static PDF form offered by NCIIPC, CERT-In and NIC-CERT. It is also recommended that forms for vulnerability reporting are made available in a variety of Indic languages for improved accessibility.

- **Standardisation of Processes:** Entities that are responsible for receiving and resolving vulnerability reports should adhere to standardised processes on vulnerability handling and disclosure (ISO 30111 & ISO 29147). If additional processes and standards are to be developed, the same should include public, multi-stakeholder consultation in order to ensure proper representation of a multitude of interests.

- **Ensuring Confidentiality of the Disclosure Process**: Bodies receiving vulnerability reports should use both transport layer and end-to-end encryption to help mitigate the risk of interception of vulnerability reports. Entities which make use of PGP should ensure that their public keys are easy to locate and access.

4. **Formalizing and Expanding Existing Processes:** A formal, continuous vulnerability disclosure or time-bound bug bounty program has not yet been introduced by the Government. The implementation of such a program, either in partnership with the private sector or through independent means, could potentially expand the scope of interaction (both quantitatively and qualitatively) between the Government and security researchers. Such a programme could be developed in conjunction with the four entities that are currently tasked with receiving vulnerability reports and could also expand to include other relevant Government departments. As described in the paper, there are several models which have proven to be successful for Governments around the world, including time-bound bug bounty challenges that are open to groups of selected individuals, and/or continual vulnerability disclosure programs for specific arms of the Government, which would be more inclusive in terms of participation and thus would enable a consistent stream of vulnerability report submissions.

5. **Removal of Legislative Barriers:** Our research found that there are multiple reforms that can strengthen the legal regime enabling strong collaborations between hackers and the Government. Such reforms will reduce areas of legal ambiguity and potential penalization for legitimate actions and ensure enforcement of existing provisions. These include **legal exceptions for security research**:

   - As of now, the scope of the provisions and foundational definitions are broad enough to penalise activities undertaken by security researchers. A clear distinction needs to be drawn between (i) actions with no malicious motive (eg. accidently transmitting malware or viruses to a computer system), (ii) research into vulnerabilities and exploits undertaken in good faith, and (iii) the malicious exploitation of security vulnerabilities.[50] There should be broad legislative exception for individuals, security researchers and practitioners. For instance, the transmission of malware samples across networks should not, in itself, be a civil or criminal offence. The exceptions should be carved into Section 43, Section 65 Section 66. Such exceptions exist in certain laws in foreign jurisdictions: for example, the Digital Millennium Copyright Act

[50] Katie Moussouris, *Vulnerability Disclosure Deja Vu: Prosecute Crime Not Research*, Dark Reading **https://www.darkreading.com/vulnerabilities---threats/vulnerability-disclosure-deja-vu-prosecute-crime-not-research/a/d-id/1320384**

has an exemption from liability on reverse engineering and security research if done in good faith.[51]

- Under the rules issued for each computer system notified as "Critical Information Infrastructure" under Section 70 of the Act, the Government can explore the addition of a testing notice procedure. Through such a procedure, security researchers who wish to actively look for vulnerabilities in critical information infrastructure would first have to seek permission from the maintainers of a particular system in order to undertake the testing process.[52] The researchers would be bound to an agreed upon time frame, and the procedure could additionally mandate that security researchers adhere to the practice of coordinated disclosure with respect to any vulnerabilities that may be discovered.

[51] US Copyright Office, Library of Congress, *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies* **https://s3.amazonaws.com/public-inspection.federalregister.gov/2015-27212.pdf**

[52] *Such a procedure shall only be applicable to "active" attempts at discovering bugs or security vulnerabilities in critical information infrastructure and shall not be applicable to vulnerabilities discovered during the regular course of accessing and using a system.*