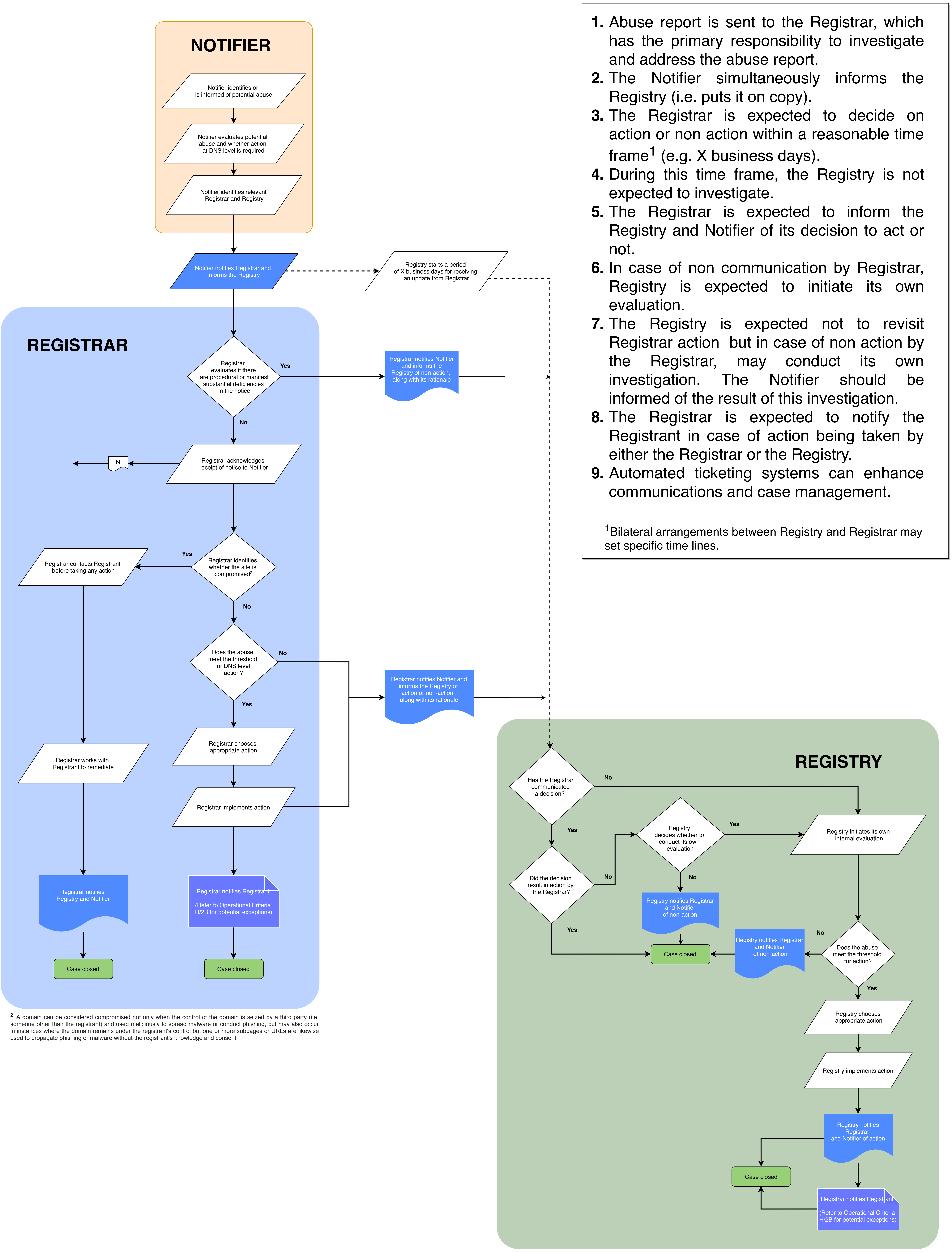
ADDRESSING PHISHING AND MALWARE: A PROCEDURAL WORKFLOW

REF: 20-115 I November 2, 2020

INTERNET & JURISDICTION POLICY NETWORK

This workflow maps the respective roles of Notifiers, Registrars and Registries and the sequence of their interactions.


NOTIFIER
Notifier identifies or is informed of potential abuse
Notifier evaluates potential abuse and whether action at DNS level is required
Notifier identifies relevant Registrar and Registry
Notifier notifies Registrar and informs the Registry
Registry starts a period of X business days for receiving an update from Registrar
REGISTRAR
Registrar evaluates if there are procedural or manifest substantial deficiencies in the notice
Yes
Registrar notifies Notifier and informs the Registry of non-action, along with its rationale
No
Registrar acknowledges receipt of notice to Notifier
N
Registrar identifies whether the site is compromised²
Yes
Registrar contacts Registrant before taking any action
Registrar works with Registrant to remediate
Registrar notifies Registry and Notifier
Case closed
No
Does the abuse meet the threshold for DNS level action?
No
Registrar notifies Notifier and informs the Registry of action or non-action, along with its rationale
Yes
Registrar chooses appropriate action
Registrar implements action
Registrar notifies Registrant
(Refer to Operational Criteria H/2B for potential exceptions)
Case closed
REGISTRY
Has the Registrar communicated a decision?
No
Registry initiates its own internal evaluation
Yes
Did the decision result in action by the Registrar?
No
Registry decides whether to conduct its own evaluation
Yes
No
Registry notifies Registrar and Notifier of non-action.
Yes
Case closed
Does the abuse meet the threshold for action?
No
Registry notifies Registrar and Notifier of non-action
Yes
Registry chooses appropriate action
Registry implements action
Registry notifies Registrar and Notifier of action
Case closed
Registrar notifies Registrant
(Refer to Operational Criteria H/2B for potential exceptions)

1. Abuse report is sent to the Registrar, which has the primary responsibility to investigate and address the abuse report.
2. The Notifier simultaneously informs the Registry (i.e. puts it on copy).
3. The Registrar is expected to decide on action or non action within a reasonable time frame[1] (e.g. X business days).
4. During this time frame, the Registry is not expected to investigate.
5. The Registrar is expected to inform the Registry and Notifier of its decision to act or not.
6. In case of non communication by Registrar, Registry is expected to initiate its own evaluation.
7. The Registry is expected not to revisit Registrar action but in case of non action by the Registrar, may conduct its own investigation. The Notifier should be informed of the result of this investigation.
8. The Registrar is expected to notify the Registrant in case of action being taken by either the Registrar or the Registry.
9. Automated ticketing systems can enhance communications and case management.

[1] Bilateral arrangements between Registry and Registrar may set specific time lines.

[2] A domain can be considered compromised not only when the control of the domain is seized by a third party (i.e. someone other than the registrant) and used maliciously to spread malware or conduct phishing, but may also occur in instances where the domain remains under the registrant's control but one or more subpages or URLs are likewise used to propagate phishing or malware without the registrant's knowledge and consent.