Findings and Recommendations regarding the OSI election of Spring 2021

OSI Oversight Committee
2 July 2021

Background

The Open Source Initiative (OSI) conducts an annual election for its board of directors. However, this actually comprises two separate elections, one for each of the two classes of membership and board seat: Individual and Affiliate. Each class of membership elects distinctly separate seats on the board, and members are only permitted to vote for candidates in their respective class. For example, an OSI Affiliate may only vote in the Affiliate election which, in turn, only consists of candidates for the “Affiliate seats” on the Board itself. For more information about this system, please see: https://opensource.org/elections.

In the process of tabulating the Spring 2021 election, a member of the OSI’s staff discovered that a ballot that had been issued to an Affiliate member’s email address had been cast in the Individual election. This breaks with the rule that Affiliates may only vote in the Affiliate election as outlined above. This was especially significant because the provisional Individual election results had a margin of a single vote.

Because it was unclear how this might have happened (or if there might have been other incorrect ballots or irregularities), officers of the OSI Board recommended that the OSI re-run its Spring 2021 election in order to maintain the integrity of the process. Upon discussion and investigation, however, the Board decided to bring in a separate temporary and Oversight Committee (OC) to oversee a forensic investigation into precisely what had happened as well as to provide recommendations back to the OSI Board.
Findings

Summary

The Oversight Committee finds that a chain of events — one triggering the decision to re-run the election and several others discovered throughout the subsequent forensic investigation — warrants re-running both the Spring 2021 Individual and Affiliate elections. This should only be performed once OSI has remedied various administrative processes around the handling of data and corrected several errors within its database and systems.

Details

Contrary to the initially issued statement about a “vulnerability”, there is no known security vulnerability in OSI’s voting processes. Rather, there were several weaknesses in its internal processes and access controls that combined in cause of events.

To begin with, many people had write access to CiviCRM (the customer relationship management tool used by the OSI) including both staff and members of the board. Internal historical norms within OSI allowed board members to routinely edit contact details in CiviCRM, including data that can affect eligibility to vote in Individual elections. This access had been granted in the past due to the (former) involvement of board members in the organization’s day-to-day operations.

This particular weakness allowed a board member to update CiviCRM data shortly before the Spring 2021 election in such a way as to create the conditions for an Affiliate organization to be incorrectly marked as eligible to vote in the Individual election. This could happen because the electoral roll (the list of individuals and organisations who will be sent their ballots) is generated from CiviCRM, as it is this system is intended to represent the single point of truth regarding who is eligible to vote as well as the email address to send ballots to. To be clear, there is no indication or evidence to suggest that this update to CiviCRM was made with the intention to cause an extra ballot to be improperly issued. Indeed, we found no evidence that the board member intended to trigger the improper issuance of the ballot, or even that the board member would have a reason to know their edit would cause the ballot to be issued in the first place. But it was nonetheless this change to contact details that led to OSI’s system incorrectly generating a ballot.

In fact, nine ballots were incorrectly issued in the Individual election to entities who were not eligible to vote in that election. Of these nine ballots, however, only one ballot was actually cast. This particular ballot was the one issued as a result of the edit of CiviCRM data (as described
above) and forensic work indicates that it was emailed to an organizational “role” alias that may have been accessed by a number of people. Access to this address included a current OSI board member who, coincidentally, was the board member who updated the organizational record in CiviCRM. This was discovered through a cooperative interview with the organization’s management in order to determine what might have happened. However, we do not know for certain who cast the ineligible ballot.

Helios is the electronic voting platform used by OSI to conduct its elections. In a subsequent review of Helios’ records for the Individual election, the IP address logs show that the ballot issued in error and the proper ballot for that individual were cast five minutes apart from the same IP address. Interviews with the organization suggested this was an extraordinarily busy time for staff, and no one could reasonably recall how it might have been cast.

There is no indication that this incorrectly-issued ballot was cast with any intent to deceive or cheat in the election. Indeed, the Oversight Committee holds that it is reasonable for somebody receiving a ballot via email to assume the ballot is valid and that casting it is therefore entirely permissible. In fact, the Helios voting system explicitly reminds voters that they can revise previously-cast ballots if they wish, serving to underscore this related belief.

The above paragraphs have outlined how the OSI issued ballots in the Individual election to parties who should not have received them. However, forensic work shows that the OSI also failed to send ballots to a number of individual members who were eligible to vote. As a result of internal data handling errors, OSI therefore deprived some members of their ability to vote. In any case, the results of the Individual election were close enough that either (a) the one miscast ballot or (b) any of the non-sent ballots may have affected the outcome of the Individual election.

There were also errors in issuing ballots for the separate election for Affiliate seats of the Board. In this election, each Affiliate should have received one ballot at that Affiliate’s associated contact email address, but some Affiliates did not receive their ballot at all. Furthermore, other Affiliates received multiple ballots, each sent to a different contact email address at that Affiliate. In five such cases, Affiliate ballots were cast that should not have been.

Unfortunately, the Oversight Committee received this forensic information late in its review process and therefore did not have a chance to contact Affiliates who had received duplicate ballots to investigate further. It is therefore unclear exactly how many discrepancies exist between the list of Affiliate voters who were sent ballots and Affiliates who were actually eligible to vote. In any event, it is clear that some Affiliate ballots were miscast and that a number of Affiliates members of the OSI were disenfranchised. If the Oversight Committee had a longer period in which to do its work, it would have investigated the Affiliate election in more detail to provide more detail for the OSI Board. Given the need to provide OSI with faster information to support decision-making about running new elections, the Oversight Committee decided to leave that future work to the discretion of the Board.
Conclusions

The Oversight Committee (OC) concludes that the OSI was justified in its decision to recall the Spring 2021 election as well as to engage an outside expert in order to examine this specific election along with its underlying systems and processes.

As a result of this examination, the OC concludes that a chain of events — one triggering the decision to re-run the election and several others discovered throughout the subsequent forensic investigation — warrants re-running both the Individual and Affiliate elections. These elections should, of course, only be performed once OSI has remedied various administrative processes surrounding data handling and corrected several errors in its database and systems. Remediating these systems and data management deficiencies (as outlined in the forensic report) should restore the OSI’s ability to run accurate elections as well as meet their obligation to ensure integrity for its Individual and Affiliate members.

Whilst OSI had publicly stated that a "vulnerability" had been exploited (and thus potentially implying an external attack), the issue was ultimately situated in how data was internally managed. In particular, there is no indication or evidence that any ballot was cast with any intent to deceive or cheat in the election. Rather, it was a result of a patchwork of system integrations and policies that no longer suit the OSI in its current evolution towards a more mature and professionally-staffed organization. It may be helpful to note that in the OC’s discussions with the consultant that conducted the forensic investigation, they noted that the types of data hygiene and access issues that he identified are typical for small, non-profit organizations.

Recommendations

1. Re-run both the Individual and Affiliate election with the correct list of eligible voters, correcting both the inadvertent omissions and inadvertent additions to the electoral rolls. This should only be done after addressing all of the errors identified in the forensic report.

2. From now on, stagger the running of Individual and Affiliate elections. The Oversight Committee encountered significant human and technical confusion between the two elections throughout its investigation. Running the Affiliate and Individual elections at different times will help reduce confusion surrounding the roles and types of ballots by both the OSI and its membership.

3. Decrease the number of people who have write access to CiviCRM. At the time of discovery, board member access to CiviCRM was temporarily revoked — this should remain a permanent operations policy.
4. Deploy better logging and data retention to support any future forensic research.


6. Release a summary version of the audit report to the public, omitting any Personally Identifiable Information (PII) where appropriate.

7. The Board should consider whether there is value in conducting a deeper investigation into the improperly cast Affiliate ballots. This would provide details about the Affiliate election similar to those uncovered about the Individual election.

Methodology

The Oversight Committee (OC) was charged with reviewing the facts and reports from the Spring election and to make recommendations to the board in order to remedy any issues that arose as a result.

The OC was given access and opportunity to review the investigation by the independent forensic expert in addition to all records and reports related to the election. The OC met privately several times, collaborated via email and also met with the President of the OSI and JMA Consulting who was tasked with performing the forensic analysis. The OC also interviewed management from the Affiliate organization whose ballot should not have been cast in the Individual election.

Committee members who accepted the invitation to volunteer included several OSI Board members (who were not standing for office in the election) as well as members of the broader open source community known to our membership to be neutral and trustworthy. The Oversight Committee Members were: Deb Bryant (board member); Chris Lamb (board member); James Vasile (OSI member); Liz Fong-Jones (OSI member); and Stefano Zacchiroli (OSI member).